```
File  16:Gale Group PROMT(R) 1990-2005/Jul 21
         (c) 2005 The Gale Group
File 148:Gale Group Trade & Industry DB 1976-2005/Jul 22
         (c)2005 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 275:Gale Group Computer DB(TM) 1983-2005/Jul 22
         (c) 2005 The Gale Group
File 621:Gale Group New Prod.Annou.(R) 1985-2005/Jul 22
         (c) 2005 The Gale Group
File 636:Gale Group Newsletter DB(TM) 1987-2005/Jul 21
         (c) 2005 The Gale Group
File   9:Business & Industry(R) Jul/1994-2005/Jul 21
         (c) 2005  The Gale Group
File  15:ABI/Inform(R) 1971-2005/Jul 22
         (c) 2005 ProQuest Info&Learning
File  20:Dialog Global Reporter 1997-2005/Jul 22
         (c) 2005 The Dialog Corp.
File  95:TEME-Technology & Management 1989-2005/Jun W2
         (c) 2005 FIZ TECHNIK
File 476:Financial Times Fulltext 1982-2005/Jul 22
         (c) 2005 Financial Times Ltd
File 610:Business Wire 1999-2005/Jul 21
         (c) 2005 Business Wire.
File 613:PR Newswire 1999-2005/Jul 22
         (c) 2005 PR Newswire Association Inc
File 624:McGraw-Hill Publications 1985-2005/Jul 22
         (c) 2005 McGraw-Hill Co. Inc
File 634:San Jose Mercury  Jun 1985-2005/Jul 21
         (c) 2005 San Jose Mercury News
File 810:Business Wire 1986-1999/Feb 28
         (c) 1999 Business Wire
File 813:PR Newswire 1987-1999/Apr 30
         (c) 1999 PR Newswire Association Inc
File  88:Gale Group Business A.R.T.S. 1976-2005/Jul 21
         (c) 2005 The Gale Group
File 647:CMP  Computer Fulltext 1988-2005/Jul W1
         (c) 2005 CMP Media, LLC
File 674:Computer News Fulltext 1989-2005/Jul W3
         (c) 2005 IDG Communications
File 696:DIALOG Telecom. Newsletters 1995-2005/Jul 21
         (c) 2005 The Dialog Corp.
File 369:New Scientist 1994-2005/May W3
         (c) 2005 Reed Business Information Ltd.
File 484:Periodical Abs Plustext 1986-2005/Jul W3
         (c) 2005 ProQuest
File 370:Science 1996-1999/Jul W3
         (c) 1999 AAAS
File 553:Wilson Bus. Abs. FullText 1982-2004/Dec
         (c) 2005 The HW Wilson Co

Set     Items   Description
S1      48731   DIGITAL()RIGHT? ? OR DRM OR DIGITAL()RIGHT?()MANAGEMENT
S2    7134200   COPYRIGHT? OR INTELLECTUAL()PROPERT???
S3      17734   (S1 OR S2)(5N)(CRYPT? OR ENCIPH? OR ENCYPH? OR DECRYPT? OR
             CODE OR CODES OR CODING? OR CIPHER? OR CYPHER? OR ENCRYPT? OR
             ENCOD?)
S4          3   (S1 OR S2)(5N)(RE()ENCRYPT? OR REENCRYPT?)
S5      83280   (TRANSFER? OR DISTRIBUT? OR DOWNLOAD? OR UPLOAD? OR PLAYBA-
             CK OR PLAY()BACK OR (UP OR DOWN)()LOAD?)(5N)(CRYPT? OR ENCIPH?
              OR ENCYPH? OR DECRYPT? OR CODE OR CODES OR CODING? OR CIPHER?

Sylvia Keys                    22-Jul-05 02:40 PM
```

```
              OR CYPHER? OR ENCRYPT? OR ENCOD?)
S6      318422   (MULTI OR MULTIPLE OR MANY OR SEVERAL OR PLURAL? OR NUMERO-
            US)(5N)KEY? ?
S7       98134   (FIRST OR PRIMARY OR SECOND?)(3N)KEY? ?
S8        3311   SECRET()KEY? ?
S9         411   AU=(SAITO, M? OR SAITO M?)
S10      99518   S3 OR S4 OR S5
S11        307   S10(S)(S6 OR S7)
S12          9   S11(S)S8
S13          1   S12 NOT PY>1994
S14         18   S11 NOT PY>1994
S15         17   S14 NOT S13
S16         17   S15 NOT PY>1994
S17         15   RD (unique items)
S18          0   S9(S)(S3 OR S4)
```

13/3,K/1 (Item 1 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

00759575 94-08967
A public key extension to the Common Cryptographic Architecture
Le, An V; Matyas, Stephen M; Johnson, Donald B; Wilkins, John D
IBM Systems Journal v32n3 PP: 461-485 1993
ISSN: 0018-8670 JRNL CODE: ISY
WORD COUNT: 16326

...TEXT: cannot be accomplished without involving the KDC each time an initial key is to be **distributed** .

With public key **cryptography** , electronic **distribution** of initial keys is more feasible and economical using a simple, widely known protocol. When ...

...been proposed for certifying and registering public keys, and for improving the integrity of the **key** distribution process.(17,20) **Many** of these methods require the involvement of trusted certification centers or authentication seers whose roles are similar to those of key distribution centers in **secret** - **key** -based key distribution. Even with that requirement, public-key-based key distribution is still considered more advantageous than **secret** - **key** -based key distribution.(17,18,21) The advantages are these. **First** , with public- **key** -based key distribution, the certification center or the authentication server can be off line and key distribution is still possible. In contrast, with **secret** - **key** -based key distribution, on-line access to a key distribution center is usually needed each time the communicating parties establish an initial keying relationship. **Second** , in public- **key** -based key distribution, the degree of trust placed on the central authority (e.g., a...

...center) is generally less than the degree of trust placed on the central authority in **secret** - **key** -based key distribution. This is because with distributed public keys, one needs to be concerned only with their integrity, whereas with distributed **secret** **keys** (i.e., DEA keys), one is concerned with both the secrecy and the integrity of...

17/3,K/1 (Item 1 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

02799487 Supplier Number: 43759153 (USE FORMAT 7 FOR FULLTEXT)
The industry goes 'back to school'
National Home Center News, v0, n0, p23
April 5, 1993
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 1112

... being sponsored by a leading home center chain, which he also declined to reveal, and **several** **key** manufacturers, **distributors** and bar- **code** scanning equipment vendors in the wood products industry.
To gather information about bar coding, Vlosky...

17/3,K/2 (Item 1 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

07576164 SUPPLIER NUMBER: 16270847 (USE FORMAT 7 OR 9 FOR FULL TEXT)
CyberSource sells software on Internet. (CyberSource Corp's software.net service)
Rodriguez, Karen
InfoWorld, v16, n47, p53(1)
Nov 21, 1994
ISSN: 0199-6649 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 442 LINE COUNT: 00037

... customer's PC. For security, encryption is used in transmitting programs over the Internet; customers **first** **download** the password **key** to **decrypt** , then the software.
Users can preview software programs by downloading product demonstrations. The service also...

17/3,K/3 (Item 1 from file: 160)
DIALOG(R)File 160:Gale Group PROMT(R)

01619204
WESTERN DIGITAL'S NEW LOW-COST, LOW-POWER DATA ENCRYPTION DEVICE THOROUGHLY SECURES DATA.
NEWS RELEASE April 20, 1987 p. 11

... It will be used in any applications that require on- line, end-to-end data **encryption** / **decryption** such as electronic funds **transfers** , secure brokerage transactions and automatic teller data transfers. The WD20C03 has two modes of operation...

... decrypt the data. In Cipher Block Chaining mode, the WD20C03 uses the same 56-bit **key** but adds a **second** variable called an initial vector. Both key and user-assigned initial vector are used to...

17/3,K/4 (Item 1 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

01264428 SUPPLIER NUMBER: 07782550
XDOS runs on Unix machines. (product announcement)
Danca, Richard A.
Federal Computer Week, v3, n34, p38(2)
August 21, 1989
DOCUMENT TYPE: product announcement ISSN: 0893-052X LANGUAGE: ENGLISH RECORD TYPE: ABSTRACT

...ABSTRACT: a computer-aided software engineering tool called the analyzer to create a key disk that **uploads** the DOS binary **code** into a Unix machine then runs XDOS' converter. Hunter has created **key** disks for **many** popular programs and workstations. The company will license the analyzer.

17/3,K/5 (Item 2 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

01213402 SUPPLIER NUMBER: 04683846 (USE FORMAT 7 OR 9 FOR FULL TEXT)
T1 encryption plan protects data. (connectivity section)
Kopeck, Ron
PC Week, v4, n9, pC9(2)
March 3, 1987
ISSN: 0740-1604 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 1498 LINE COUNT: 00124

... the same key at exactly the same time.
The DOD does not permit contractors to **download** **encryptor** / **decryptor** keys; units must be loaded with keys directly. Said Kirby Dickson, telecommunications security manager for have **many** individuals know the **keys** or how the keys are changed.
Also, Hughes was concerned that incorrect key definitions between...

17/3,K/6 (Item 1 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)

01881357 Supplier Number: 43252676 (USE FORMAT 7 FOR FULLTEXT)
Background on Mass-Market Encryption Software Issue
Export Control News, v6, n8, pN/A
August 27, 1992
Language: English Record Type: Fulltext
Document Type: Newsletter; Trade
Word Count: 479

... nothing to restrict its availability abroad but instead diminishes the international competitiveness of US companies.
Several **key** software manufacturers, such as Microsoft, worked through SPA to lobby Congress to include an amendment in H.R. 3489, a bill to reauthorize the EAA, that would mandate the **transfer** of mass-market **encryption** software to the jurisdiction of the Commerce Department. Before Congress adjourned, the bill was virtually...

17/3,K/7 (Item 2 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)

01012165 Supplier Number: 40335552 (USE FORMAT 7 FOR FULLTEXT)
Most companies fail software test
Advanced Military Computing, v4, n7, pN/A
March 28, 1988
Language: English Record Type: Fulltext
Document Type: Newsletter; Trade
Word Count: 849

... an aside. He noted the management of the maturation of Ada compilers will be a **key** task for the Ada community. **Many** compilers have come under fire for being too slow and generating poor **code** .

17/3,K/8 (Item 1 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

00773318 94-22710
Placement of cryptographic key distribution within OSI: Design alternatives and assessment
Fumy, Walter; Leclerc, Matthias
Computer Networks & ISDN Systems v26n2 PP: 217-225 Oct 1993
ISSN: 0376-5075 JRNL CODE: CNI

...ABSTRACT: key management is to provide procedures for handling cryptographic keying material to be used by **cryptographic** mechanisms. Even though **many key distribution** protocols have been designed, little attention has been devoted to the question of how those...

17/3,K/9 (Item 2 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

00609491 92-24594
Retailers, Manufacturers Applaud Quick Response
Hoffman, Thomas
Computerworld v26n15 PP: 15 Apr 13, 1992
ISSN: 0010-4841 JRNL CODE: COW
WORD COUNT: 503

...TEXT: 500 million.

MANY REWARDS

Partnering companies have been able to maximize Quick Response by using **several key** technologies, including electronic data interchange (EDI), electronic funds **transfer** , electronic payments and various bar- **coding** and scanning technologies. Retailers benefit from lower costs, reduced inventories, streamlined ordering and receiving processes...

17/3,K/10 (Item 3 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

00527040 91-01384
"Do-It-Yourself" Cryptography

Carroll, John M.
Computers & Security v9n7 PP: 613-619 Nov 1990
ISSN: 0167-4048 JRNL CODE: CSC

...ABSTRACT: CRYPTO-LEGGO (CLEG), a stream cipher, may be an inexpensive alternative to using the Data **Encryption** Standard (DES), chips **distributed** under the Commercial Communications Security Endorsement Program, or products from vendors with close ties to...

...by adding or removing program modules without altering their essential formats. The ciphers use so **many** **keys** that each implementation is a distinct cipher system. Tests suggest that either cipher can provide...

17/3,K/11 (Item 4 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

00412879 88-29712
Small Switches with Big Features Face Full Market
Hunter, John
Network World v5n29 PP: 1, 41-43, 51-52 Jul 18, 1988
ISSN: 0887-7661 JRNL CODE: NWW

...ABSTRACT: digital network (ISDN). Pricing wars are expected to shake out weaker competitors. Hybrid switches combine **many** features of **key** systems with the advanced functionality of PBXs and are appealing as a low-cost solution...

...will be offering networking PBXs. Meanwhile, many vendors have responded to user needs with account **coding** and fairly powerful automatic call **distribution** . Observers note that PBXs have become commodity-like, and prices are expected to fall soon.

17/3,K/12 (Item 1 from file: 810)
DIALOG(R)File 810:Business Wire

0001022 BW170

OAK INDUSTRIES: Closes $23,000,000 sale of Sigma Units to Maclean Hunter

January 15, 1986

Byline: Business Editors

...date,
Sigma provies to be extremely reliable and provides superior signal security.
Sigma employs audio **encryption** utilizing a **multi** -level **key** **distribution** technique and **encrypts** video decoding commands. The advanced technology of the Sigma product line from Oak is far...

17/3,K/13 (Item 1 from file: 88)
DIALOG(R)File 88:Gale Group Business A.R.T.S.

03377816 SUPPLIER NUMBER: 16504690

Trust in the new information age.
Maher, David P.
AT & T Technical Journal, v73, n5, p9(8)
Sept-Oct, 1994
ISSN: 8756-2324 LANGUAGE: English RECORD TYPE: Abstract

...ABSTRACT: must guarantee authenticity of identity, confidentiality, integrity, validity of remittances and service availability. Digital signatures, **encryption** systems and certificate-based **key distribution** systems can solve **many** of these problems.

17/3,K/14 (Item 2 from file: 88)
DIALOG(R)File 88:Gale Group Business A.R.T.S.
(c) 2005 The Gale Group. All rts. reserv.

01505682 SUPPLIER NUMBER: 03054247
Another promising code falls; a code that looked too good to be true has a fatal weakness and now can be broken in a few seconds.
Kolata, Gina
Science, v222, p1224(1)
Dec 16, 1983
CODEN: SCIEAS ISSN: 0036-8075 LANGUAGE: English
RECORD TYPE: Fulltext
WORD COUNT: 851 LINE COUNT: 00081

... the discrete exponentials code unsatisfactory for practical use. At Mitre, computer scientists were using the **code** to **distribute encoding** keys for a more traditional cryptographic system, the DES, that was used to scramble messages...

...the discrete exponentials code is 127 bits and it takes, says Schanning, less than 10 **seconds** to exchange DES **keys** with it. "If we had to go to 241 bits, it would take minutes and...

17/3,K/15 (Item 1 from file: 484)
DIALOG(R)File 484:Periodical Abs Plustext
(c) 2005 ProQuest. All rts. reserv.

00919792
Schrodinger's Catflap
Stewart, Ian
Nature (GNAA), v353 n6343, p384-385, p.2
Oct 3, 1991
ISSN: 0028-0836 JOURNAL CODE: GNAA
DOCUMENT TYPE: News
LANGUAGE: English RECORD TYPE: Abstract
LENGTH: Long (31+ col inches)

ABSTRACT: Quantum cryptography, an emerging science, shows how quantum theory can be used to guarantee secure **distribution** of a **cryptographic key** . **Several** recent developments in the field are discussed.
?

```
File 256:TecInfoSource 82-2005/Jun
         (c) 2005 Info.Sources Inc
File   2:INSPEC 1969-2005/Jul W2
         (c) 2005 Institution of Electrical Engineers
File  35:Dissertation Abs Online 1861-2005/Jun
         (c) 2005 ProQuest Info&Learning
File  65:Inside Conferences 1993-2005/Jul W3
         (c) 2005 BLDSC all rts. reserv.
File  99:Wilson Appl. Sci & Tech Abs 1983-2005/Jun
         (c) 2005 The HW Wilson Co.
File 583:Gale Group Globalbase(TM) 1986-2002/Dec 13
         (c) 2002 The Gale Group
File 474:New York Times Abs 1969-2005/Jul 21
         (c) 2005 The New York Times
File 475:Wall Street Journal Abs 1973-2005/Jul 21
         (c) 2005 The New York Times
File   8:Ei Compendex(R) 1970-2005/Jul W2
         (c) 2005 Elsevier Eng.  Info. Inc.
File  94:JICST-EPlus 1985-2005/May W5
         (c)2005 Japan Science and Tech Corp(JST)
File   6:NTIS 1964-2005/Jul W2
         (c) 2005 NTIS, Intl Cpyrght All Rights Res
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File  34:SciSearch(R) Cited Ref Sci 1990-2005/Jul W3
         (c) 2005 Inst for Sci Info

Set     Items   Description
S1       2897   DIGITAL()RIGHT? ? OR DRM OR DIGITAL()RIGHT?()MANAGEMENT
S2     336777   COPYRIGHT? OR INTELLECTUAL()PROPERT???
S3       1466   (S1 OR S2)(5N)(CRYPT? OR ENCIPH? OR ENCYPH? OR DECRYPT? OR
             CODE OR CODES OR CODING? OR CIPHER? OR CYPHER? OR ENCRYPT? OR
             ENCOD?)
S4          0   (S1 OR S2)(5N)(RE()ENCRYPT? OR REENCRYPT?)
S5      29108   (TRANSFER? OR DISTRIBUT? OR DOWNLOAD? OR UPLOAD? OR PLAYBA-
             CK OR PLAY()BACK OR (UP OR DOWN)()LOAD?)(5N)(CRYPT? OR ENCIPH?
              OR ENCYPH? OR DECRYPT? OR CODE OR CODES OR CODING? OR CIPHER?
              OR CYPHER? OR ENCRYPT? OR ENCOD?)
S6      22044   (MULTI OR MULTIPLE OR MANY OR SEVERAL OR PLURAL? OR NUMERO-
             US)(5N)KEY? ?
S7       6482   (FIRST OR PRIMARY OR SECOND?)(3N)KEY? ?
S8       3069   SECRET()KEY? ?
S9      20758   AU=(SAITO, M? OR SAITO M?)
S10     30504   S3 OR S5
S11       172   S10 AND (S6 OR S7)
S12        29   S11 AND S8
S13         4   S12 NOT PY>1994
S14         0   S9 AND S3
```

13/5/1 (Item 1 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

03847799 E.I. No: EIP94041266443
Title: Bulk encryption algorithm for use with RSA
Author: Sewell, R.F.
Source: Electronics Letters v 29 n 25 Dec 9 1993. p 2183-2185
Publication Year: 1993
CODEN: ELLEAK ISSN: 0013-5194
Language: English
Document Type: JA; (Journal Article) Treatment: T; (Theoretical)
Journal Announcement: 9406W2
Abstract: The public key cryptosystem known as RSA is widely presumed to be secure but in software implementations is slow and even in hardware implementations encryption with a general 512 bit exponent runs only at tens of kilobits per second. Due to this, use of a **second** , fast, **secret key** , cryptosystem such as DES as the bulk encryption method is common while the session key for the system is **transferred** using RSA. Use of two **encryption** systems increases the security risk as breaking either RSA or DES is sufficient to obtain the knowledge of the plaintext thus it is desirable to use a fast **secret - key** bulk encryption algorithm whose security can be demonstrably related to that of RSA. This paper presents discussions about a proposed system designated as QS to achieving this goal. 24 Refs.
Descriptors: *Cryptography; Information theory; Security of data; Computer software; Algorithms; Computer hardware; **Encoding** (symbols); Data **transfer** ; Data communication systems
Identifiers: Bulk encryption algorithm; Cryptosystem; **Secret key** ; Cryptanalytic activity; Hardware encryption; Quisquater and Couvreur method ; Session key
Classification Codes:
716.1 (Information & Communication Theory); 723.2 (Data Processing); 723.1 (Computer Programming); 722.3 (Data Communication, Equipment & Techniques)
716 (Radar, Radio & TV Electronic Equipment); 723 (Computer Software); 722 (Computer Hardware)
71 (ELECTRONICS & COMMUNICATIONS); 72 (COMPUTERS & DATA PROCESSING)

13/5/2 (Item 2 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

03664126 E.I. No: EIP93050804067
Title: On the design of conference key distribution systems for the broadcasting networks
Author: Laih, Chi-Sung; Yen, Sung-Ming
Corporate Source: Nat Cheng Kung Univ, Tainan, Taiwan
Conference Title: Proceedings of the 12th Annual Joint Conference of the IEEE Computer and Communications Societies - IEEE INFOCOM '93
Conference Location: San Francisco, CA, USA Conference Date: 19930330-19930401
E.I. Conference No.: 18536
Source: Proceedings - IEEE INFOCOM v 3 1993. Publ by IEEE, IEEE Service Center, Piscataway, NJ, USA. p 1406-1413
Publication Year: 1993
CODEN: PINFEZ ISSN: 0743-166X ISBN: 0-8186-3580-0
Language: English
Document Type: CA; (Conference Article) Treatment: T; (Theoretical); A;

(Applications)
Journal Announcement: 9308W4
Abstract: There are two important parts in the design of modern cryptographic systems. The first part is the design of cryptosystems. The other is the design of key distribution systems. The former constitutes the main portion of data protection operation while the latter dominates the soul of the cryptosystem, i.e., the encryption and decryption keys. In this paper, we propose a design methodology of conference - key distribution system based on the threshold scheme for the broadcasting networks. We show that if a conference chairman can share a **secret key** with each of the other conference participants then any threshold scheme can be used to construct a conference - key distribution system (CKDS). Since there already exist **many** ID - based **key** distribution systems for two users to share a common **secret key** , we can therefore easily construct the ID - based CKDS for the broadcasting networks. (Author abstract) 17 Refs.

Descriptors: *Cryptography; Broadcasting; Security of data; Information theory
Identifiers: Key **distribution** systems; Broadcasting networks; Data protection; **Encryption** keys; Decryption keys
Classification Codes:
723.5 (Computer Applications); 716.1 (Information & Communication Theory)
723 (Computer Software); 716 (Radar, Radio & TV Electronic Equipment)
72 (COMPUTERS & DATA PROCESSING); 71 (ELECTRONICS & COMMUNICATIONS)

13/5/3 (Item 3 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

02837394 E.I. Monthly No: EIM8912-048641
Title: Authenticated group key distribution scheme for a large distributed network.
Author: Harn, Lein; Kiesler, Thomas
Corporate Source: Univ of Missouri, Kansas City, MO, USA
Conference Title: Proceedings: 1989 IEEE Symposium on Security and Privacy
Conference Location: Oakland, CA, USA Conference Date: 19890501
Sponsor: IEEE, Technical Committee on Security and Privacy, New York, NY, USA; Int Assoc for Cryptologic Research
E.I. Conference No.: 12565
Source: Proceedings of the Symposium on Security and Privacy May 1989. Publ by IEEE, IEEE Service Center, Piscataway, NJ, USA. Available from IEEE Service Cent (cat n 89CH2703-7), Piscataway, NJ, USA. p 300-309
Publication Year: 1989
CODEN: PSSPEO
Language: English
Document Type: PA; (Conference Paper) Treatment: G; (General Review); T ; (Theoretical)
Journal Announcement: 8912
Abstract: The authors propose a decentralized key distribution scheme. In this scheme, there are as **many** local **key** centers as needed and each user needs to select a key center at which to register when first joining the network. The most significant feature of the method is that each center needs only a single **secret key** . All personal keys that it needs for delivering encrypted keys to groups of users can be derived from this single key through a one-way function. 14 Refs.
Descriptors: *DATA PROCESSING--*Security of Data; COMPUTER SYSTEMS, DIGITAL--Distributed; MATHEMATICAL MODELS; COMPUTER NETWORKS
Identifiers: AUTHENTICATION; DECENTRALIZED KEY **DISTRIBUTION** ; **ENCRYPTED** KEYS
Classification Codes:
723 (Computer Software)
72 (COMPUTERS & DATA PROCESSING)

13/5/4 (Item 4 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

01848562 E.I. Monthly No: EIM8501-002831
Title: DOES PUBLIC KEY CRYPTOGRAPHY PROVIDE ADEQUATE COMMUNICATION SECURITY?
Author: Desmedt, Y.; Vandewalle, J.; Govaerts, R.
Corporate Source: Catholic Univ of Louvain, ESAT Lab, Heverlee, Belg

Conference Title: Conference Proceedings - Electronics for National Security.
Conference Location: Brussels, Belg Conference Date: 19830927
Sponsor: Cahners Exposition Group, Des Plaines, IL, USA; Cahners Exposition Group S. A. , Guildford, Engl
E.I. Conference No.: 05642
Source: Publ by Interavia Publ Group, Geneva, Switz p 52-59
Publication Year: 1983
Language: English
Document Type: PA; (Conference Paper)
Journal Announcement: 8501
Abstract: One of the major problems in data communication systems protected by classical **cryptography** is the **distribution** of the **secret keys** between all senders and receivers. Such a distribution becomes even impractical in large, especially international networks. The public key algorithm is considered that should solve the problem of key distribution and at the same time provide electronic signatures for documents such as contracts. The idea of public **key** and its conditions are explained. **Several** criticisms on the practical aspects are discussed such as: transmission speed, loosing keys, security. 45 refs.
Descriptors: *DATA PROCESSING--*Security of Data; COMPUTERS--Data Communication Systems
Identifiers: PUBLIC KEY CRYPTOGRAPHY; **SECRET KEYS** ; INTERNATIONAL COMMUNICATION NETWORKS; TRANSMISSION SPEED; KEY LOSS; KEY DISTRIBUTION
Classification Codes:
723 (Computer Software); 716 (Radar, Radio & TV Electronic Equipment); 718 (Telephone & Line Communications)
72 (COMPUTERS & DATA PROCESSING); 71 (ELECTRONICS & COMMUNICATIONS)
?

```
File 344:Chinese Patents Abs Aug 1985-2005/May
         (c) 2005 European Patent Office
File 347:JAPIO Nov 1976-2005/Feb(Updated 050606)
         (c) 2005 JPO & JAPIO
File 350:Derwent WPIX 1963-2005/UD,UM &UP=200546
         (c) 2005  Thomson Derwent
File 348:EUROPEAN PATENTS 1978-2005/Jul W02
         (c) 2005 European Patent Office
File 349:PCT FULLTEXT 1979-2005/UB=20050721,UT=20050714
         (c) 2005 WIPO/Univentio
File 331:Derwent WPI First View    UD=200546
         (c) 2005  Thomson Derwent
File 371:French Patents 1961-2002/BOPI 200209
         (c) 2002 INPI.  All rts. reserv.

Set     Items   Description
S1       2320   DIGITAL()RIGHT? ? OR DRM OR DIGITAL()RIGHT?()MANAGEMENT
S2    2275225   COPYRIGHT? OR INTELLECTUAL()PROPERT???
S3       7782   (S1 OR S2)(5N)(CRYPT? OR ENCIPH? OR ENCYPH? OR DECRYPT? OR
             CODE OR CODES OR CODING? OR CIPHER? OR CYPHER? OR ENCRYPT? OR
             ENCOD?)
S4         28   (S1 OR S2)(5N)(RE()ENCRYPT? OR REENCRYPT?)
S5      45417   (TRANSFER? OR DISTRIBUT? OR DOWNLOAD? OR UPLOAD? OR PLAYBA-
             CK OR PLAY()BACK OR (UP OR DOWN)()LOAD?)(5N)(CRYPT? OR ENCIPH?
              OR ENCYPH? OR DECRYPT? OR CODE OR CODES OR CODING? OR CIPHER?
              OR CYPHER? OR ENCRYPT? OR ENCOD?)
S6      28620   (MULTI OR MULTIPLE OR MANY OR SEVERAL OR PLURAL? OR NUMERO-
             US)(5N)KEY? ?
S7      22732   (FIRST OR PRIMARY OR SECOND?)(3N)KEY? ?
S8       6789   SECRET()KEY? ?
S9      18787   AU=(SAITO, M? OR SAITO M?)
S10     52310   S3 OR S4 OR S5
S11       358   S10(3N)(S6 OR S7)
S12       139   S11 AND S8
S13        59   S12 AND IC=G06F
S14        56   S13 NOT (MULTIPLE()ADDRESS?)
S15        34   S9 AND (S3 OR S4)
```

14/3,K/1 (Item 1 from file: 347)
DIALOG(R)File 347:JAPIO
(c) 2005 JPO & JAPIO. All rts. reserv.

06018908 **Image available**
DATA CONTENTS DISTRIBUTION SYSTEM

PUB. NO.: 10-302008 [JP 10302008 A]
PUBLISHED: November 13, 1998 (19981113)
INVENTOR(s): SAITO MAKOTO
APPLICANT(s): MITSUBISHI CORP [000597] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 09-126357 [JP 97126357]
FILED: April 30, 1997 (19970430)

INTL CLASS: **G06F-017/60** ; **G06F-005/00** ; **G06F-015/00** ; H04L-009/08

ABSTRACT

...work data contents by making a second user decode a ciphered scenario by using a **secret key** and reconstitute the work data contents based on a decoded work scenario...

... presents the digitally signed work program to a copyright management center 8 and requests a **second secret key** for decoding the **ciphered** source data contents component. The **copyright** management center 8 transfers the second **secret key** to the second user in the case that a first user is the appropriate user of the source data contents for which the second **secret key** is requested. Then, the second user decodes the ciphered scenario by using the **secret key** and reconstitutes the work data contents based on the decoded work scenario.

14/3,K/2 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2005 Thomson Derwent. All rts. reserv.

010625430 **Image available**
WPI Acc No: 1996-122383/199613
XRPX Acc No: N96-102820
Code key delivery method for delivering code key through public circuit - involves checking random number received from terminal with that generated in key centre for producing code key from key centre
Patent Assignee: NIPPON TELEGRAPH & TELEPHONE CORP (NITE)
Inventor: KANAI A; MIYAKE N; MORIYASU K; OKUYAMA H; TERAUCHI A
Number of Countries: 002 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 8018552	A	19960119	JP 95105063	A	19950428	199613	B
US 5651066	A	19970722	US 95431407	A	19950428	199735	
JP 3348753	B2	20021120	JP 95105063	A	19950428	200282	

Priority Applications (No Type Date): JP 9491857 A 19940428
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 8018552	A		21	H04L-009/06	
US 5651066	A		22	H04L-009/00	
JP 3348753	B2		21	H04L-009/32	Previous Publ. patent JP 8018552

...Abstract (Basic): the key centre. A decoder (21) in the key centre decodes K3 by using a **secret key** K2d. A coder (22) enciphers a random number K4 by K3 and sends it to...

...Abstract (Equivalent): method of cipher key distribution in a system formed by a key center having a **cipher key** to be **distributed** and a **plurality** of user terminals connected with the key center through a public network, the method comprising...
International Patent Class (Additional): **G06F-015/00** ...

14/3,K/3 (Item 1 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01898247
Systems and methods for secure transaction management and electronic rights protection
Systeme und Verfahren zur Verwaltung von gesicherten Transaktionen und zum Schutz von elektronischen Rechten
Systemes et procedes pour gerer des transactions securisees et pour proteger des droits electroniques
PATENT ASSIGNEE:
Intertrust Technologies Corp., (2434320), 460 Oakmead Parkway, Sunnyvale, CA 94086-4708, (US), (Applicant designated States: all)
INVENTOR:
Ginter, Karl L., 10404 43rd Avenue, Beltsville, Maryland 20705, (US)
Shear, Victor H., 5203 Battery Lane, Bethesda, Maryland 20814, (US)
Spahn, Francis J., 2410 Edwards Avenue, El Cerrito, California 94530, (US)
Van Wie, David M., 1250 Lakeside Drive, Sunnyvale, California 94086, (US)
LEGAL REPRESENTATIVE:
Smith, Norman Ian et al (36041), fJ CLEVELAND 40-43 Chancery Lane, London WC2A 1JQ, (GB)
PATENT (CC, No, Kind, Date): EP 1531379 A2 050518 (Basic)
APPLICATION (CC, No, Date): EP 2004078195 960213;
PRIORITY (CC, No, Date): US 388107 950213
DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
RELATED PARENT NUMBER(S) - PN (AN):
EP 861461 (EP 96922371)

NTERNATIONAL PATENT CLASS: **G06F-001/00 ; G06F-017/60**
ABSTRACT WORD COUNT: 151
NOTE:
Figure number on first page: 75

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200520	173
SPEC A	(English)	200520	167172
Total word count - document A			167345
Total word count - document B			0
Total word count - documents A + B			167345

INTERNATIONAL PATENT CLASS: **G06F-001/00** ...

... **G06F-017/60**

...SPECIFICATION they believe appropriate to their business requirements.
VDE offers an architecture that avoids reflecting specific **distribution** biases, administrative and control perspectives, and content types. Instead, VDE provides a broad-spectrum, fundamentally... other information in order to, for example, reduce frequency of access by an SPU to **secondary** storage 652 and/or for other reasons. Dual ported external RAM can be particularly effective...which the metering/transaction management functionality is incorporated).
The third approach is distinct from the **first** two in that it does not incorporate VDE functionality associated with metering/transaction management and...

14/3,K/4 (Item 2 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01888484
Systems and methods for secure transaction management and electronic rights protection
Systeme und Verfahren zur gesicherten Transaktionsverwaltung und elektronischem Rechtsschutz
Systemes et procedes de gestion de transactions securisees et de protection de droits electroniques
PATENT ASSIGNEE:
ELECTRONIC PUBLISHING RESOURCES, INC., (976840), 460 Oakmead Parkway, Sunnyvale, CA 94086-4708, (US), (Applicant designated States: all)
INVENTOR:
Ginter, Karl L., 10404 43rd Avenue, Beltsville, Maryland 20705, (US)
Shear, Victor H., 5203 Battery Lane, Bethesda, Maryland 20814, (US)
Spahn, Francis J., 2410 Edwards Avenue, El Cerrito, California 94530, (US)
Van Wie, David M., 1780 East 25th Avenue, Eugene, OR 97403, (US)
LEGAL REPRESENTATIVE:
Smith, Norman Ian et al (36041), fJ CLEVELAND 40-43 Chancery Lane, London WC2A 1JQ, (GB)
PATENT (CC, No, Kind, Date): EP 1526472 A2 050427 (Basic)
APPLICATION (CC, No, Date): EP 2004078254 960213;
PRIORITY (CC, No, Date): US 388107 950213
DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
RELATED PARENT NUMBER(S) - PN (AN):

EP 861461 (EP 96922371)
INTERNATIONAL PATENT CLASS: **G06F-017/60 ; G06F-009/46**
ABSTRACT WORD COUNT: 151
NOTE:
Figure number on first page: 75

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200517	355
SPEC A	(English)	200517	167222
Total word count - document A			167577
Total word count - document B			0
Total word count - documents A + B			167577

INTERNATIONAL PATENT CLASS: **G06F-017/60 ...**

... G06F-009/46

...SPECIFICATION most usage, audit, reporting, payment, and distribution control methods are themselves at least in part **encrypted** and are executed by the secure subsystem of a VDE installation. Thus, for example, billing...100.

Almost any sort of transaction you can think of can be supported by virtual **distribution** environment 100. A few of **many** examples of transactions that can be supported by virtual distribution environment 100 include:

C home...The subservice concept extends to supporting multiple processors, multiple SPEs 503, multiple HPEs 655, and **multiple** communications services.

The preferred embodiment ROS 602 provides the following RPC based service providers/requestors...

14/3,K/5 (Item 3 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01869029
Systems and methods for secure transaction management and electronic rights protection
Systeme und Verfahren zur gesicherten Transaktionsverwaltung und elektronischem Rechtsschutz
Systemes et procedes de gestion de transactions securisees et de protection de droits electroniques
PATENT ASSIGNEE:
ELECTRONIC PUBLISHING RESOURCES, INC., (976840), 460 Oakmead Parkway, Sunnyvale, CA 94086-4708, (US), (Applicant designated States: all)
INVENTOR:
Ginter, Karl L., 10404 43rd Avenue, Beltsville, Maryland 20705, (US)
Shear, Victor H., 5203 Battery Lane, Bethesda, Maryland 20814, (US)
Spahn, Francis J., 2410 Edwards Avenue, El Cerrito, California 94530, (US)
Van Wie, David M., 1250 Lakeside Drive, Sunnyvale, California 94086, (US)
LEGAL REPRESENTATIVE:
Smith, Norman Ian et al (36041), fJ CLEVELAND 40-43 Chancery Lane, London WC2A 1JQ, (GB)
PATENT (CC, No, Kind, Date): EP 1515216 A2 050316 (Basic)
EP 1515216 A3 050323
APPLICATION (CC, No, Date): EP 2004078194 960213;

PRIORITY (CC, No, Date): US 388107 950213
DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
RELATED PARENT NUMBER(S) - PN (AN):
EP 861461 (EP 96922371)
INTERNATIONAL PATENT CLASS: **G06F-001/00** ; **G06F-017/60**
ABSTRACT WORD COUNT: 144
NOTE:
Figure number on first page: 75C

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200511	276
SPEC A	(English)	200511	167210
Total word count - document A			167486
Total word count - document B			0
Total word count - documents A + B			167486

INTERNATIONAL PATENT CLASS: **G06F-001/00** ...
... **G06F-017/60**

...SPECIFICATION they believe appropriate to their business requirements. VDE offers an architecture that avoids reflecting specific **distribution** biases, administrative and control perspectives, and content types. Instead, VDE provides a broad-spectrum, fundamentally... most usage, audit, reporting, payment, and distribution control methods are themselves at least in part **encrypted** and are executed by the secure subsystem of a VDE installation. Thus, for example, billing...The

subservice concept extends to supporting multiple processors, multiple SPEs 503, multiple HPEs 655, and **multiple** communications services. The preferred embodiment ROS 602 provides the following RPC based service providers/requestors...

14/3,K/6 (Item 4 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01845538
Method and system for key distribution comprising a step of authentication and a step of key distribution using a KEK (key encryption key)
Verfahren und System zur Schlusseldistribution mit einem Authentifizierungschritt und einem Schlusseldistributionsschritt unter Verwendung von KEK (key encryption key)
Methode et systeme de distribution de cle comprenant une etape **d'authentification et une de distribution de cle a l'aide de KEK (key encryption key)**
PATENT ASSIGNEE:
Eisst Limited, (4500220), 6-8 Underwood Street, London N17 JQ, (GB), (Applicant designated States: all)
INVENTOR:
Ronchi, Corrado, Via Masaccio 1, 00196 Roma, (IT)
Zakhidov, Shukhrat, 6 O.Zakirova St., Apt. 57, Tashkent 700000, (UZ)
LEGAL REPRESENTATIVE:
Gervasi, Gemma, Dr. (40515), Notarbartolo & Gervasi S.p.A., Corso di Porta Vittoria, 9, 20122 Milano, (IT)
PATENT (CC, No, Kind, Date): EP 1501238 A1 050126 (Basic)
APPLICATION (CC, No, Date): EP 2003016787 030723;

DESIGNATED STATES: AT; BE; BG; CH; CY; CZ; DE; DK; EE; ES; FI; FR; GB; GR; HU; IE; IT; LI; LU; MC; NL; PT; RO; SE; SI; SK; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK
INTERNATIONAL PATENT CLASS: H04L-009/30; H04L-009/32; **G06F-001/00**
ABSTRACT WORD COUNT: 207
NOTE:
Figure number on first page: 3

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200504	1249
SPEC A	(English)	200504	3790
Total word count - document A			5039
Total word count - document B			0
Total word count - documents A + B			5039

...INTERNATIONAL PATENT CLASS: **G06F-001/00**

...ABSTRACT A1
A method for protecting the **transfer** and storage of data by **encryption** using a private **key** encrypted with a **first key** encrypting **key** , which is encrypted using a second key encrypting key. This latter key is encrypted using...

...SPECIFICATION to be transferred is typically first encrypted by a symmetric encryption algorithm using a pseudorandom **secret key** . The **secret key** is then encrypted utilizing the public key of the intended recipient, and both the encrypted message and the encrypted **secret key** are transmitted to the intended recipient. When the message and **secret key** are delivered, the recipient uses the private key to decrypt the **secret key** , and then decrypts the message using the **secret key** .
The larger an encryption key, e.g. 128 bits confronted to 56 bits, the greater...

...of securing key distribution and storage, they suffer from several disadvantages inherent in storing the **secret key** (s) and data either on a centralized server database or on a device in the...

...device.
Firstly, it is possible that the storage devices may be probed to obtain the **secret key** (s). This is particularly true in the case the key storage is kept on the...

...manner that it can be shown that only the authorised user can access all the **secret keys** required for the processing of a particular message or data.

Summary of the invention
It...

...yet another object of the present invention to provide a method and system for defeating **secret key** discovery attacks in a distributed key cryptography system.
The foregoing objects are achieved by means...

14/3,K/7 (Item 5 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01776084
Reconfigurable secure input device
Rekonfigurierbares sicheres Eingabegerat
Dispositif reconfigurable securise d'entree de donnees
PATENT ASSIGNEE:
Minebea Co., (4687790), Arco Tower, 19th Floor, 1-8-1, Shimo-Meguro, Meguro-ku, Tokyo 153-8662, (JP), (Applicant designated States: all)
INVENTOR:
Fauble, Charles, 18309 Oakmont Drive No. 925, Canyon Country, California 91387, (US)
Dickerman, Robert, 938 Azalea Drive, Costa Mesa California 92626, (US)
Takeda, Toshisada, 2716 Simi Hills Lane, Simi Valley, California 93063, (US)
LEGAL REPRESENTATIVE:
Every, David Aidan et al (74581), MARKS & CLERK, Sussex House, 83-85 Mosley Street, Manchester M2 3LG, (GB)
PATENT (CC, No, Kind, Date): EP 1447734 A2 040818 (Basic)
APPLICATION (CC, No, Date): EP 2004250504 040130;
PRIORITY (CC, No, Date): US 359780 030207
DESIGNATED STATES: AT; BE; BG; CH; CY; CZ; DE; DK; EE; ES; FI; FR; GB; GR; HU; IE; IT; LI; LU; MC; NL; PT; RO; SE; SI; SK; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK
INTERNATIONAL PATENT CLASS: **G06F-001/00**
ABSTRACT WORD COUNT: 140
NOTE:
Figure number on first page: 004

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200434	1491
SPEC A	(English)	200434	9137
Total word count - document A			10628
Total word count - document B			0
Total word count - documents A + B			10628

INTERNATIONAL PATENT CLASS: **G06F-001/00**

...SPECIFICATION key encryption and public-key encryption. Symmetric-key encryption requires that each computer have a **secret key** . The **secret key** is used to encode and decode the information transmitted between the two computers. In order for symmetric-key encryption to work, the **secret key** must be provided to each of the two computers. If this is done over a non-secure transmission line, the security of the **secret key** may be compromised and someone may be able to intercept the **secret key** .
Public-key encryption utilizes a combination of a private key and a public key. The...

...utilize the random number generator to generate a pseudo-random session key, which is a **secret key** . If the second computing device generates the **secret key** , the second computing device transmits the **secret key** to the first computing device utilizing public-private key cryptography.
After the **secret key** is shared between the first computing device and second computing device, symmetric cryptography, using the **secret key** , is performed because the computational burden is lower on the system than with public key...

...bits. In some cases, the public-private key cryptography is utilized only to share the **secret key** . In some systems, it may also be required that digital signatures are necessary during the...

...transformation instruction to the global network 46.
The first computing device 42 may receive the **second** computing device public **key** and the **encrypted** transformation instruction(s) and may **transfer** the **second** computing device public **key** and the encrypted transformation instruction(s) to an RSID 50. The RSID 50 may store...

...output and placed in a temporary buffer. The transformed code may be encrypted utilizing the **second** computing device public **key** and the **encrypted** transformed **code** may be **transferred** from the RSID 50 to the first computing device 42. The first computing device 42...

14/3,K/8 (Item 6 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01752676
Systems and methods for secure transaction management and electronic rights protection
Systeme und Verfahren zur gesicherten Transaktionsverwaltung und elektronischem Rechtsschutz
Systemes et procedes de gestion de transactions securisees et de protection de droits electroniques
PATENT ASSIGNEE:
ELECTRONIC PUBLISHING RESOURCES, INC., (976840), 460 Oakmead Parkway, Sunnyvale, CA 94086-4708, (US), (Applicant designated States: all)
INVENTOR:
Ginter, Karl L., 10404 43rd Avenue, Beltsville Maryland 20705, (US)
Shear, Victor H., 5203 Battery Lane, Bethesda Maryland 20814, (US)
Spahn, Francis J., 2410 Edwards Avenue, El Cerrito California 94530, (US)
van Wie, David M., 1250 Lakeside Drive, Sunnyvale California 94086, (US)
LEGAL REPRESENTATIVE:
Smith, Norman Ian et al (36041), fJ CLEVELAND 40-43 Chancery Lane, London WC2A 1JQ, (GB)
PATENT (CC, No, Kind, Date): EP 1431864 A2 040623 (Basic)
EP 1431864 A3 050216
APPLICATION (CC, No, Date): EP 2004075701 960213;
PRIORITY (CC, No, Date): US 388107 950213
DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
RELATED PARENT NUMBER(S) - PN (AN):
EP 861461 (EP 96922371)
INTERNATIONAL PATENT CLASS: **G06F-001/00** ; **G06F-017/60**
ABSTRACT WORD COUNT: 151
NOTE:
Figure number on first page: 77

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200426	1450
SPEC A	(English)	200426	166929
Total word count - document A			168379
Total word count - document B			0
Total word count - documents A + B			168379

INTERNATIONAL PATENT CLASS: **G06F-001/00 ...**

... G06F-017/60

14/3,K/9 **(Item 7 from file: 348)**
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2005 European Patent Office. All rts. reserv.

01679172
Systems and methods for issuing usage licenses for digital content and services
System und Methode zum Ausstellen von Verwendungslizenen fur digitale Inhalte und Dienste
Systemes et methodes permettant de generer des licences d'utilisation de contenu numerique et de services
PATENT ASSIGNEE:
MICROSOFT CORPORATION, (749866), One Microsoft Way, Redmond, WA 98052, (US), (Applicant designated States: all)
INVENTOR:
Waxman, Peter, 10008 NE 28th Place, Bellevue, Washington 98004, (US)
Narin, Attilla, 8741 NE 144th Court, Bothell, Washington 98011, (US)
Cottrille, Scott, 22618 NE 14th Drive, Sammamish, Washington 98074, (US)
Krishnaswamy, Vinay, 23319 NE 142nd Place, Woodinville, Washington 98072, (US)
DeMello, Marco A., 6606 152nd Ave., Redmond, Washington 98052, (US)
Venkatesh, Chandramouli, 414 213th Place SE, Sammamish, Washington 98074, (US)
Byrum, Frank D., 1200 Western Ave.No.1210, Seattle, Washington 98101, (US)
Bourne, Steve, 303 E.Pike Street No.602, Seattle, Washington 98122, (US)
LEGAL REPRESENTATIVE:
Grunecker, Kinkeldey, Stockmair & Schwanhausser Anwaltssozietat (100721), Maximilianstrasse 58, 80538 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1378811 A2 040107 (Basic)
APPLICATION (CC, No, Date): EP 2003013556 030613;
PRIORITY (CC, No, Date): US 185511 020628
DESIGNATED STATES: AT; BE; BG; CH; CY; CZ; DE; DK; EE; ES; FI; FR; GB; GR; HU; IE; IT; LI; LU; MC; NL; PT; RO; SE; SI; SK; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK
INTERNATIONAL PATENT CLASS: **G06F-001/00**
ABSTRACT WORD COUNT: 181
NOTE:
Figure number on first page: 3

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200402	2069
SPEC A	(English)	200402	12669
Total word count - document A			14738
Total word count - document B			0
Total word count - documents A + B			14738

INTERNATIONAL PATENT CLASS: **G06F-001/00**

...SPECIFICATION used to encrypt the digital content. Symmetric key algorithms, which are sometimes referred to as " **secret key** " algorithms, use the same key to decrypt a message as they do to encrypt the...

...CLAIMS claim 26, wherein encrypting the content encryption key comprises:
retrieving the public key from the **digital rights management** server;
generating a **second** content 1encryption key ;
encrypting the content encryption key using the second content encryption key; and
encrypting the second...

14/3,K/10 (Item 8 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01654782
Contents distribution scheme using tamper-resistant processor
Schema zur Verteilung des Inhalts mit Hilfe eines betrugssicheren Prozessors
Un schema de distribution de contenu au moyen d'un processeur inviolable
PATENT ASSIGNEE:
Kabushiki Kaisha Toshiba, (2077102), 1-1, Shibaura 1-chome, Minato-ku, Tokyo 105-8001, (JP), (Applicant designated States: all)
INVENTOR:
Isozaki, Hiroshi, c/o Int. Prop. Division, Toshiba Corporation, 1-1 Shibaura 1-chome, Minato-ku, Tokyo, (JP)
Hashimoto, Mikio, c/o Int. Prop. Division, Toshiba Corporation, 1-1 Shibaura 1-chome, Minato-ku, Tokyo, (JP)
LEGAL REPRESENTATIVE:
Midgley, Jonathan Lee (85971), Marks & Clerk 57-60 Lincoln's Inn Fields, GB-London WC2A 3LS, (GB)
PATENT (CC, No, Kind, Date): EP 1361497 A2 031112 (Basic)
EP 1361497 A3 041117
APPLICATION (CC, No, Date): EP 2003252895 030509;
PRIORITY (CC, No, Date): JP 2002134507 020509
DESIGNATED STATES: AT; BE; BG; CH; CY; CZ; DE; DK; EE; ES; FI; FR; GB; GR; HU; IE; IT; LI; LU; MC; NL; PT; RO; SE; SI; SK; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK
INTERNATIONAL PATENT CLASS: **G06F-001/00**
ABSTRACT WORD COUNT: 92
NOTE:
Figure number on first page: 1

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200346	1666
SPEC A	(English)	200346	12733
Total word count - document A			14399
Total word count - document B			0
Total word count - documents A + B			14399

INTERNATIONAL PATENT CLASS: **G06F-001/00**

...ABSTRACT the contents receiving and viewing program by using either the public key algorithm or the **secret key** algorithm, and transmits the contents by trusting the reception device only when that authentication succeeds.

...SPECIFICATION contents distribution scheme utilizing a device adopting a

tamperresistant processor which internally maintains a processor **secret key** .

DESCRIPTION OF THE RELATED ART

In recent years, due to the spread of computer networks...

...a microprocessor and a reception device having a tamper resistant microprocessor which maintains a processor **secret key** inside and an external memory, the tamper resistant microprocessor being capable of obtaining a **plurality** of program **keys** by **decrypting** a **plurality** of **distribution keys** respectively corresponding to a **plurality** of programs by using the processor **secret key** , and executing the plurality of programs arranged in the external memory in a state of...a prescribed public key algorithm based on a public key that is corresponding to a **secret key** of the contents receiving and viewing program and maintained in advance by the contents transmission program, or by a **secret key** algorithm based on a **secret key** that is maintained in advance by the contents transmission program and shared with the contents...

...method executed by a transmission device having a tamper resistant microprocessor which maintains a processor **secret key** inside and an external memory, and a reception device, the tamper resistant microprocessor being capable of obtaining a **plurality** of program **keys** by **decrypting** a **plurality** of **distribution keys** respectively corresponding to a **plurality** of programs by using the processor **secret key** , and executing the plurality of programs arranged in the external memory in a state of...

...of programs by using respectively corresponding program keys, the contents distribution method comprising: storing a **secret key** that is set in correspondence to the contents transmission device, in a state of being...

...a prescribed public key algorithm based on a public key that is corresponding to the **secret key** of the contents transmission program and maintained in advance by a contents receiving and viewing...

...contents transmission program only when it is proved that the contents transmission program has the **secret key** at the authenticating step, by the contents receiving and viewing program.

According to another aspect...

...device and a reception device each having a tamper resistant microprocessor which maintains a processor **secret key** inside and an external memory, the tamper resistant microprocessor being capable of obtaining a **plurality** of program **keys** by **decrypting** a **plurality** of **distribution keys** respectively corresponding to a **plurality** of programs by using the processor **secret key** , and executing the plurality of programs arranged in the external memory in a state of...

...a microprocessor and a reception device having a tamper resistant microprocessor which maintains a processor **secret key** inside and an external memory, the tamper resistant microprocessor being capable of obtaining a **plurality** of program **keys** by **decrypting** a **plurality** of **distribution keys** respectively corresponding to a **plurality** of programs by using the processor **secret key** , and executing the plurality of programs arranged in the external memory in a state of...

...a prescribed public key algorithm based on a public key that is corresponding to a **secret** key of the contents receiving and viewing program and maintained in advance by the contents transmission program,

...

14/3,K/11 (Item 9 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01574894
Encrypted program distribution system using computer network
System zur Verteilung eines verschlusselten Programms durch ein Netzwerk
Systeme de distribution de logiciels criptes utilisant un reseau informatique
PATENT ASSIGNEE:
Kabushiki Kaisha Toshiba, (2077102), 1-1, Shibaura 1-chome, Minato-ku, Tokyo 105-8001, (JP), (Applicant designated States: all)
INVENTOR:
Hashimoto, Mikio, c/o Intell. Prop. Division, Toshiba Corporation, 1-1, Shibaura 1-chome, Minato-ku, Tokyo, (JP)
Shirakawa, Kenji, c/o Intell. Prop. Division, Toshiba Corporation, 1-1, Shibaura 1-chome, Minato-ku, Tokyo, (JP)
Shimojo, Yoshimitsu, c/o Intell. Prop. Division, Toshiba Corporation, 1-1, Shibaura 1-chome, Minato-ku, Tokyo, (JP)
Teramoto, Keiichi, c/o Intell. Prop. Division, Toshiba Corporation, 1-1, Shibaura 1-chome, Minato-ku, Tokyo, (JP)
Fujimoto, Kensaku, c/o Intell. Prop. Division, Toshiba Corporation, 1-1, Shibaura 1-chome, Minato-ku, Tokyo, (JP)
Ozaki, Satoshi, c/o Intell. Prop. Division, Toshiba Corporation, 1-1, Shibaura 1-chome, Minato-ku, Tokyo, (JP)
LEGAL REPRESENTATIVE:
Granleese, Rhian Jane (92091), Marks & Clerk, 57-60 Lincoln's Inn Fields, London WC2A 3LS, (GB)
PATENT (CC, No, Kind, Date): EP 1308820 A2 030507 (Basic)
EP 1308820 A3 030709
APPLICATION (CC, No, Date): EP 2001309273 011031;
PRIORITY (CC, No, Date): JP 2000332068 001031
DESIGNATED STATES: DE; FR; GB
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: **G06F-001/00**
ABSTRACT WORD COUNT: 138
NOTE:

Figure number on first page: 1

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200319	3876
SPEC A	(English)	200319	12193
Total word count - document A			16069
Total word count - document B			0
Total word count - documents A + B			16069

INTERNATIONAL PATENT CLASS: **G06F-001/00**

...SPECIFICATION codes and data by hardware. Its safety level depends on the safety level of the **secret key** embedded in the processor chip.
However, in this type of tamper resistant processor, different unique
...configured to decrypt the execution file received by the second receiving unit by using a **secret key** corresponding to the public key.

According to another aspect of the present invention there is...

...configured to encrypt at least a part of the execution file by using a prescribed **secret key** , when the source file passes an examination by the examination unit; a public key receiving...

...an examination by the examination unit; a second encryption unit configured to encrypt the prescribed **secret key** by using the public key received by the public key receiving unit, when the source...

...configured to send the execution file encrypted by the first encryption unit and the prescribed **secret key** encrypted by the second encryption unit to the execution file receiving device, when the source...
...distribution device; a second receiving unit configured to receive the execution file and the prescribed **secret key** sent from the encrypted program distribution device; and a first decryption unit configured to decrypt the prescribed **secret key** received by the second receiving unit by using a **secret key** corresponding to the public key; and a second decryption unit configured to decrypt the execution file received by the second receiving unit by using the prescribed **secret key** decrypted by the first decryption unit.

According to another aspect of the present invention there...

...configured to encrypt at least a part of the execution file by using a prescribed **secret key** , when the source file passes an examination by the examination unit; a public key receiving...an examination by the examination unit; a second encryption unit configured to encrypt the prescribed **secret key** by using the public key received by the public key receiving unit, when the source...

...configured to send the execution file encrypted by the first encryption unit and the prescribed **secret key** encrypted by the second encryption unit to the execution file receiving device, when the source...

...device; and (i) decrypting the execution file received by the step (h) by using a **secret key** corresponding to the public key at the execution file receiving device.

According to another aspect...

...c); (e) encrypting at least a part of the execution file by using a prescribed **secret key** , at the encrypted program distribution device, when the source file passes an examination by the...

...when the source file passes an examination by the step (c); (g) encrypting the prescribed **secret key** by using the public key received by the step (f), at the encrypted program distribution...

...step (c); (h) sending the execution file encrypted by the step (e) and the prescribed **secret key** encrypted by the step (g) from the encrypted program distribution device to the execution file...

...passes an examination by the step (c); (i) receiving the execution file and the prescribed **secret key** sent from the encrypted program distribution device at the execution file receiving device; (j) decrypting the prescribed **secret key** received by the step (i) by using a **secret key** corresponding to the public key at the execution file receiving device; and (k) decrypting the execution file received by the step (i) by using the prescribed **secret key** decrypted by the step (j) at the execution file receiving device.

According to another aspect...b); (d) encrypting at least a part of the execution file by using a prescribed **secret key** , when the source file

the...

14/3,K/12 (Item 10 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01529241
Digital work protection system, recording medium apparatus, transmission apparatus, and playback apparatus
System zum Schutz digitaler Inhalte, Aufzeichnungsgerat, Ubertragungsgerat und Wiedergabegerat
Systeme de protection de contenu numerique, appareil d'enregistrement, appareil de transmission et appareil de reproduction
PATENT ASSIGNEE:
MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD., (216883), 1006, Oaza-Kadoma, Kadoma-shi, Osaka 571-8501, (JP), (Applicant designated States: all)
INVENTOR:
Harada, Shunji, 2-20-52, Tamadenishi, Nishinari, Osaka-fu 557-0045, (JP)
Futa, Yuichi, 3-7-36, Diatou-cho, Miyakojima-ku, Osaka-shi, Osaka-fu 534-0002, (JP)
Miyazaki, Masaya, 1-6-14, Asahigaoka, Ikeda-shi, Osaka-fu, 563-0022, (JP)
Sekibe, Tsutomu, 5-49-34, Yamanoue, Hirakata-shi, Osaka-fu, 573-0047, (JP)
Nakanishi, Yoshiaki, Matsunokiryo 305, 2-4-10, Matsunoki, Suginami-ku, Tokyo-to 166-0014, (JP)
Matsuzaki, Natsume, 1-6-7-803, Aomadaninishi, Minou-shi, Osaka-fu 562-0023, (JP)
LEGAL REPRESENTATIVE:
Grunecker, Kinkeldey, Stockmair & Schwanhausser Anwaltssozietat (100721), Maximilianstrasse 58, 80538 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1276106 A1 030115 (Basic)
APPLICATION (CC, No, Date): EP 2002015287 020709;
PRIORITY (CC, No, Date): JP 2001208533 010709
DESIGNATED STATES: DE; FR; GB
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: G11B-020/00; **G06F-001/00**
ABSTRACT WORD COUNT: 107
NOTE:
Figure number on first page: 1

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200303	4070
SPEC A	(English)	200303	18349
Total word count - document A			22419
Total word count - document B			0
Total word count - documents A + B			22419

...INTERNATIONAL PATENT CLASS: **G06F-001/00**

...SPECIFICATION transmission apparatus operable to encrypt original content that is the digital work, based on a **distribution encryption key** , to generate **first encrypted** information, and transmit the generated first encrypted information via a network; the reception apparatus operable...content key, to generate encrypted content, (d) encrypt the original content key using the obtained **distribution encryption key** , to generate a **first** encrypted content **key** , and (d) transmit the first encrypted information that includes the generated encrypted content and the...

...advance the distribution decryption key and the medium unique key, (b) obtain the output first **encrypted** information, (c) **decrypt** the **first encrypted** content **key** using the **distribution decryption** key, to generate an intermediate content key, (d) encrypt the generated intermediate content key using...

...content key, to generate encrypted content, and encrypt the original content key using the obtained **distribution encryption key** , to generate a **first** encrypted content **key** ; and a transmission unit operable to transmit the encrypted content and the first encrypted content...

...unique to the recording medium apparatus; an obtaining sub-unit operable to obtain the output **encrypted** content and the output **first encrypted** content **key** ; a **decryption** sub-unit operable to **decrypt** the **first encrypted** content **key** using the **distribution decryption** key, to generate an intermediate content key; an encryption sub-unit operable to encrypt the...content key, to generate encrypted content, and encrypt the original content key using the obtained **distribution encryption key** , to generate a **first** encrypted content **key** ; and a transmission unit operable to transmit the encrypted content and the first encrypted content...

...condition information, the encryption unit may further encrypt the original usage condition key using the **distribution encryption key** , to generate a **first** encrypted usage condition **key** , and encrypts the usage condition information using the original usage condition key, to generate first...

...the stated construction, use of the public key can be limited in accordance with the **secret key** being exposed, therefore content can be distributed even more safely.

Here, the storage unit may...and the transmission apparatus encrypting original content that is a digital work, based on a **distribution encryption key** , to generate **first encrypted** information, and transmitting the generated first encrypted information via a network to the reception apparatus...

...content key, to generate encrypted content, (d) encrypt the original content key using the obtained **distribution encryption key** , to generate a **first** encrypted content **key** , and (d) transmit the first encrypted information that includes the generated encrypted content and the first encrypted content key; the obtaining sub-unit may obtain the obtained first **encrypted** information; the **decryption** unit may **decrypt** the **first encrypted** content **key** using the **distribution decryption** key, to generate an intermediate content key, and generate intermediate information that includes the encrypted...

...unique to the usage condition information, (b) encrypt the original usage condition key, using the **distribution encryption key** , to generate a **first** encrypted usage condition **key** , (c) encrypt the usage condition information using the original usage condition key, to generate first...

...usage condition information via the reception apparatus, the decryption sub-unit may further decrypt the **first encrypted** usage condition **key** using the **distribution** key, to generate an intermediate usage condition key, and decrypt the first encrypted usage condition...

...using a public key generation algorithm, based on a distribution

...using a public key generation algorithm, based on a distribution decryption key that is a **secret key** , and performs encryption according to a public key encryption algorithm using a distribution encryption key...the plurality of encryption methods.

25. The recording medium apparatus of Claim 14,

wherein the **key** storage sub-unit stores a **plurality** of distribution **decryption key** candidates, and one **distribution decryption** key candidate is selected from among the **plurality** of distribution **decryption key** candidates as the distribution **decryption** key, and

the **decryption** sub-unit uses the selected **distribution decryption** key.

26. The recording medium apparatus of Claim 14,

wherein the tamper-proof module unit...

...apparatus, the transmission apparatus encrypting original content that is the digital work, based on a **distribution encryption key** , to generate **first encrypted** information, and transmits the generated first encrypted information via the network to the reception apparatus...

...content key, to generate encrypted content, (d) encrypts the original content key using the obtained **distribution encryption key** , to generate a **first** encrypted content **key** , and (e) transmits the first encrypted information that includes the generated encrypted content and the...

...advance the distribution decryption key and the medium unique key, (b) obtains the output first **encrypted** information, (c) **decrypts** the **first encrypted** content **key** using the **distribution decryption** key, to generate an intermediate content key, (d) encrypts the generated intermediate content key using...

...unique to the usage condition information, (b) encrypts the original usage condition key using the **distribution encryption key** , to generate a **first** encrypted usage condition **key** , (c) encrypts the usage condition information using the original usage condition key, to generate first reception apparatus,

the recording medium apparatus further (a) obtains via the network the **first** encrypted usage condition **key** and the **first encrypted** usage condition information, (b) **decrypts** the **first encrypted** usage condition **key** using the **distribution decryption** key, to generate an intermediate usage condition key, (c) decrypts the first encrypted usage condition...

14/3,K/13 (Item 11 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01504244
DATA ACCESS MANAGEMENT SYSTEM AND MANAGEMENT METHOD USING ACCESS CONTROL TICKET
DATENZUGRIFFSMANAGEMENTSYSTEM UND MANAGEMENTVERFAHREN MIT EINEM ZUGRIFFSSTEUERTICKET

Sylvia Keys 22-Jul-05 02:12 PM

SYSTEME DE GESTION D'ACCES AUX DONNEES ET PROCEDE DE GESTION UTILISANT UN BILLET DE COMMANDE D'ACCES

PATENT ASSIGNEE:
Sony Corporation, (214028), 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001, (JP), (Applicant designated States: all)

INVENTOR:
YOSHINO, Kenji, c/o Sony Corporation, 7-35, Kitashinagawa 6-Chome, Shinagawa-Ku, Tokyo 141-0001, (JP)
Ishibashi, Yoshihito, c/o Sony Corporation, 7-35, K itashinagawa 6-Chome, Shinagawa-Ku, Tokyo 141-0001, (JP)
SHIRAI, Taizo, c/o SONY CORPORATION, 7-35, Kitashinagawa 6-Chome, Shinagawa-Ku, Tokyo 141-0001, (JP)
TAKADA, Masayuki, c/o Sony Corporation, 7-35, Kitashinagawa 6-Chome, Shinagawa-Ku, Tokyo 141-0001, (JP)

LEGAL REPRESENTATIVE:
Robinson, Nigel Alexander Julian et al (69551), D. Young & Co., 21 New Fetter Lane, London EC4A 1DA, (GB)

PATENT (CC, No, Kind, Date): EP 1303075 A1 030416 (Basic)
WO 2002076013 020926

APPLICATION (CC, No, Date): EP 2002702791 020307; WO 2002JP2113 020307

PRIORITY (CC, No, Date): JP 200173353 010315

DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR

EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI

INTERNATIONAL PATENT CLASS: H04L-009/00; G09C-001/00; **G06F-012/14** ; **G06F-015/00** ; **G06F-017/60** ; **G06F-019/00** ; **G06F-017/00** ; G06K-019/00

ABSTRACT WORD COUNT: 137

NOTE:
Figure number on first page: 0001

LANGUAGE (Publication,Procedural,Application): English; English; Japanese

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200316	8394
SPEC A	(English)	200316	79434
Total word count - document A			87828
Total word count - document B			0
Total word count - documents A + B			87828

...INTERNATIONAL PATENT CLASS: **G06F-012/14** ...

... **G06F-015/00** ...

... **G06F-017/60** ...

... **G06F-019/00** ...

... **G06F-017/00**

...SPECIFICATION with, and that the digital signature has been generated by the entity which has the **secret key** corresponding to the public key. If the digital signature data c or d does not...

14/3,K/14 (Item 12 from file: 348)

DIALOG(R)File 348:EUROPEAN PATENTS

01504243

MEMORY ACCESS CONTROL SYSTEM AND MANAGEMENT METHOD USING ACCESS CONTROL TICKET

VORRICHTUNG ZUR SPEICHERZUGRIFFSTEUERUNG UND VERWALTUNGSVERFAHREN UNTER VERWENDUNG EINES SPEICHERZUGRIFFSTICKETS
SYSTEME DE CONTROLE D'ACCES A LA MEMOIRE ET PROCEDE DE GESTION FAISANT APPEL A UN TICKET DE CONTROLE D'ACCES
PATENT ASSIGNEE:
Sony Corporation, (214028), 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001, (JP), (Applicant designated States: all)
INVENTOR:
YOSHINO, Kenji, c/o SONY CORPORATION, 7-35, Kitashinagawa 6-chome,Shinagawa-ku,, Tokyo 141-0001, (JP)
ISHIBASHI, Yoshihito, c/o SONY CORPORATION, 7-35, Kitashinagawa 6-chome,Shinagawa-ku,, Tokyo 141-0001, (JP)
SHIRAI, Taizo, c/o SONY CORPORATION, 7-35, Kitashinagawa 6-chome,Shinagawa-ku,, Tokyo 141-0001, (JP)
TAKADA, Masayuki, c/o SONY CORPORATION, 7-35, Kitashinagawa 6-chome,Shinagawa-ku,, Tokyo 141-0001, (JP)
LEGAL REPRESENTATIVE:
Mills, Julia et al (97061), D Young & Co, 21 New Fetter Lane, London EC4A 1DA, (GB)
PATENT (CC, No, Kind, Date): EP 1276271 A1 030115 (Basic)
WO 2002076012 020926
APPLICATION (CC, No, Date): EP 2002702790 020307; WO 2002JP2112 020307
PRIORITY (CC, No, Date): JP 200173352 010315
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: H04L-009/00; G09C-001/00; **G06F-012/14** ; **G06F-015/00** ; **G06F-017/60** ; **G06F-019/00** ; G06K-017/00; G06K-019/00
ABSTRACT WORD COUNT: 119
NOTE:
Figure number on first page: 0001

LANGUAGE (Publication,Procedural,Application): English; English; Japanese
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200303	3051
SPEC A	(English)	200303	73024
Total word count - document A			76075
Total word count - document B			0
Total word count - documents A + B			76075

...INTERNATIONAL PATENT CLASS: **G06F-012/14** ...

... **G06F-015/00** ...

... **G06F-017/60** ...

... **G06F-019/00**

...SPECIFICATION with, and that the digital signature has been generated by the entity which has the **secret key** corresponding to the public key.
If the digital signature data c or d does not...for each partition.
When making an access to a file created in the partition, the **encryption** key is used for data **transfer** . There are **several** types of **encryption keys** .
For example, as shown in Fig. 85, between the device 100 and an access unit...

14/3,K/15 (Item 13 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01488671

DATA TERMINAL CAPABLE OF TRANSFERRING CIPHERED CONTENT DATA AND LICENSE ACQUIRED BY SOFTWARE

DATENENDGERAT, DAS CHIFFRIERTE INHALTSDATEN UND EINE DURCH SOFTWARE ANGESCHAFFTE LIZENZ TRANSFERIEREN KANN

TERMINAL DE DONNEES CAPABLE DE TRANSFERER DES DONNEES DE CONTENU CHIFFRE ET UNE LICENCE ACQUISES PAR L'INTERMEDIAIRE D'UN LOGICIEL

PATENT ASSIGNEE:
Sanyo Electric Co., Ltd., (2206455), 5-5, Keihan-Hondori 2-chome, Moriguchi-shi, Osaka 570-8677, (JP), (Applicant designated States: all)
FUJITSU LIMITED, (211463), 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588, (JP), (Applicant designated States: all)
Hitachi, Ltd., (204145), 6 Kanda Surugadai 4-chome, Chiyoda-ku, Tokyo 101-8010, (JP), (Applicant designated States: all)
INVENTOR:
Hori, Yoshihiro, c/o Sanyo Electric Co., Ltd, 5-5, Keihanhondori 2-chome, Moriguchi-shi, Osaka 570-8677, (JP)
Kamimura, Toru, c/o Sanyo Electric Co., Ltd, 5-5, Keihanhondori 2-chome, Moriguchi-shi, Osaka 570-8677, (JP)
Miyazono, Shinya, c/o Sanyo Electric Co., Ltd, 5-5, Keihanhondori 2-chome , Moriguchi-shi, Osaka 570-8677, (JP)
Hatakeyama, Takahisa, c/o Fujitsu Limited, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588, (JP)
Hasebe, Takayuki, c/o Fujitsu Limited, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588, (JP)
Takahashi, Masataka, c/o PFU Limited, Aza Unoke Nu98-2, Unoke-machi, Kahoku-gun, Ishikawa 929-1192, (JP)
Tsunehiro, Takashi, co/ Sys. Devel. Lab. Hitachi L, t92, Yoshida-cho, Totsuka-ku, Yokohama-shi, Kanagawa 244-0817, (JP)
Ohmori,Yoshio, c/o Denon Ltd., Sagamiharashi,, Kanagawa 228-8505, (JP)
LEGAL REPRESENTATIVE:
Glawe. Delfs. Moll (100699), Patentanwalte Postfach 26 01 62, 80058 Munchen, (DE)

PATENT (CC, No, Kind, Date): EP 1338992 A1 030827 (Basic)
WO 2002042966 020530
APPLICATION (CC, No, Date): EP 2001997765 011122; WO 2001JP10258 011122
PRIORITY (CC, No, Date): JP 2000358238 001124
DESIGNATED STATES: DE; FR; GB
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: **G06F-017/60**
ABSTRACT WORD COUNT: 114
NOTE:
Figure number on first page: 1

LANGUAGE (Publication,Procedural,Application): English; English; Japanese
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200335	2920
SPEC A	(English)	200335	23143
Total word count - document A			26063
Total word count - document B			0
Total word count - documents A + B			26063

INTERNATIONAL PATENT CLASS: **G06F-017/60**

...SPECIFICATION to the terminal or the user after being encrypted. The first is a system for **distributing** an **encryption key** for

communication, the **second** is the system for encrypting to-be-distributed contents data itself, and the third is...the license key for each memory card by providing the memory card, i.e., the **secret key** of the recording device.

Memory card 110 further includes an interface 1424 exchanging a signal ...output to the memory card, the content reproduction device or the like to which the **secret key** is leaked from the license administration module which receives the distribution.

After step S250 or...

14/3,K/16 (Item 14 from file: 348)

DIALOG(R)File 348:EUROPEAN PATENTS

01483241

INFORMATION PROCESSING APPARATUS AND METHOD, AND STORAGE MEDIUM
INFORMATIONSVERARBEITUNGSVORRICHTUNG UND VERFAHREN UND SPEICHERMEDIUM
APPAREIL ET PROCEDE DE TRAITEMENT DE DONNEES, ET SUPPORT DE STOCKAGE

PATENT ASSIGNEE:
Sony Corporation, (214028), 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001, (JP), (Applicant designated States: all)

INVENTOR:
Iino, Yoichiro, Sony Corporation, 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001, (JP)

LEGAL REPRESENTATIVE:
Horner, David Richard et al (77632), D Young & Co, 21 New Fetter Lane, London EC4A 1DA, (GB)

PATENT (CC, No, Kind, Date): EP 1365536 A1 031126 (Basic)
WO 2002069557 020906

APPLICATION (CC, No, Date): EP 2002712408 020218; WO 2002JP1337 020218

PRIORITY (CC, No, Date): JP 200150781 010226

DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR

EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI

INTERNATIONAL PATENT CLASS: H04L-009/00; **G06F-017/60**

ABSTRACT WORD COUNT: 111

NOTE:
Figure number on first page: 0007

LANGUAGE (Publication,Procedural,Application): English; English; Japanese

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200348	2347
SPEC A	(English)	200348	16823
Total word count - document A			19170
Total word count - document B			0
Total word count - documents A + B			19170

...INTERNATIONAL PATENT CLASS: **G06F-017/60**

...SPECIFICATION is possible to charge for the use of information in a form of selling the **encryption** key. For the circulation and **distribution** of the **encryption key** , in **many** cases, the encryption **key** , itself, is digitized. In this case, similarly to information to be originally distributed and sold...records included in the transfer history in order from the latest record by using a **secret key** SCA)) of the management center CA, and checks the records.

When a record which cannot...

...management center CA, the records included in the transfer history are decrypted by using a **secret key** SCA)) of the management center CA and are checked in order from the latest record...

...management center CA, the records included in the transfer history are decrypted by using a **secret key** SCA)) of the management center CA and are checked in order from the latest record...

...the public so as to be used by anybody. The decryption key is called the " **secret key** ", and is managed by a possessor so as not to leak to others. Accordingly, by...

...can transmit a code that can be decrypted only by a receiver who possesses a **secret key** .

When the public key is PK)), and the **secret key** is SK)), encryption of data M by using the public key PK)) is represented by C = E(PK)), M), and decryption of the code C by using the **secret key** SK)) is represented by M = D(SK)), C). An important property is that, by keeping the **secret key** SK)) secret, if the public key Pk)) or the code C is known, the original...

...taken into consideration. When data M exists, the creator of M uses his or her **secret key** SK)) to calculate the electronic signature SG(M) = D(Sk)), h(M)), where h() represents...

...falsified and the electronic signature SG(M) has been added by the owner of the **secret key** SK)). In other words, a message creator uses his or her **secret key** to encrypt a message, whereby a receiver of the encrypted message can decrypt the encrypted...

...an ElGamal signature, and an elliptic ElGamal signature. To avoid confusion with electronic signatures, a **secret key** SK)) for use in creating a signature is called a "signature creation key", and a...

...challenge&response authentication can be realized. By using the public key PK)), possession of the **secret key** SK)) can be confirmed without knowing the **secret key** itself. For example, a verifying side generates a random number r, calculates the value r...

...r") holds in the verifying side, it is confirmed that the other party possesses the **secret key** SK)).

Similarly, in the electronic signature technique, by using the signature verification key PK)), it...

...the signature creation key SK)).

In the challenge&response authentication, the existence of a particular **secret key** or signature creation key can be confirmed by using a corresponding public key or signature verification key, without knowing the **secret key** or signature creation key itself.

Certificate

In order to authenticate a particular other party (or...

...it is important to have a correct understanding of a public key corresponding to a **secret key** possessed by the other party, or a signature verification key corresponding to a signature creation...

...is absolutely reliable. The CA issues a certificate encrypted by using a CA's own **secret key** . In other words, the certificate cannot be freely forged by others because it bears an...by Infon)) and Pn)).

Certificate Verification

5. Content Recovering Apparatus
The recovery of content in this embodiment...

...such as a signature certificate (Infoj)), Pj)), SGj))) of the content issuing apparatus 30, a **secret key** Sj)) corresponding to a public key Pj)) included in the certificate, the public key PCA...

...recovering apparatus 50.
The electronic signature generator 56 has a function of using its own **secret key** Sj)) to generate its own electronic signature. When data M exists, the electronic signature generator 56 uses its own **secret key** Sj)) to calculate the electronic signature SG(M) = D(Sj)), h(M)) of data M...

...and that the electronic signature SG(M) has been added by the possessor of the **secret key** SK)) (as described above).
The fraud detector 59 has a function of receiving from the...by data mn)), TSGn)) is represented by D(Sn)), h(Mn)))) (where Sn)) is a **secret key** of a content holding apparatus which performs content transfer for the n-th time).
Regarding...

...SGn)) = D(SCA)), h(Infon)), Pn)))), generated by the management center CA 70 using its **secret key** SCA)), is added to a set of information linking to the content transferring side, and...

...apparatus, and nonce TNn)) (as described above).
Finally, the content transferring holding apparatus uses its **secret key** Sn)) to generate electronic signature TSGn)) for the entire transfer history including the new record...
...management center CA 70 generates a pair of a public key cryptosystem public key and **secret key** . Here, the public key of the management center CA 70 is represented by PCA')) and the **secret key** is represented by SCA)). The management center CA 70 opens only the public key PCA...

...history is verified in step (2), the operation of decrypting each record by using the **secret key** SCA)) of the management center CA 70 is added. The validity of each record is proven based on the ability to use the **secret key** SCA)) to perform proper decryption and the validity of the electronic signature in the record...

...CLAIMS predetermined management center, the records included in the transfer history are decrypted by using a **secret key** SCA)) of the management center CA and are checked in order from the latest record ...

...management center CA, the records included in the transfer history are decrypted by using a **secret key** SCA)) of the management center CA and are checked in order from the latest record...

...management center CA, the records included in the transfer history are decrypted by using a **secret key** SCA)) of the management center CA and are checked in order from the latest record...

14/3,K/17 (Item 15 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01476932

INFORMATION PROCESSING SYSTEM AND METHOD

Vorrichtung und Verfahren zur Informationsverarbeitung

SYSTEME DE TRAITEMENT DE L'INFORMATION ET PROCEDE

PATENT ASSIGNEE:
Sony Corporation, (214028), 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001, (JP), (Applicant designated States: all)

INVENTOR:
ASANO, Tomoyuki c/o SONY CORPORATION, 7-35, KITASHINAGAWA 6-CHOME SHINAGAWA-KU, Tokyo 141-0001, (JP)
OSAWA, Yoshitomo c/o SONY CORPORATION, 7-35, KITASHINAGAWA 6-CHOME SHINAGAWA-KU, Tokyo 141-0001, (JP)
OISHI, Tateo c/o SONY CORPORATION, 7-35, KITASHINAGAWA 6-CHOME SHINAGAWA-KU, Tokyo 141-0001, (JP)
ISHIGURO, Ryuji c/o SONY CORPORATION, 7-35, KITASHINAGAWA 6-CHOME SHINAGAWA-KU, Tokyo 141-0001, (JP)
TAKI, Ryuta c/o SONY CORPORATION, 7-35, KITASHINAGAWA 6-CHOME SHINAGAWA-KU, Tokyo 141-0001, (JP)

LEGAL REPRESENTATIVE:
Horner, David Richard et al (77632), D Young & Co, 21 New Fetter Lane, London EC4A 1DA, (GB)

PATENT (CC, No, Kind, Date): EP 1253739 A1 021030 (Basic)
WO 2002052781 020704

APPLICATION (CC, No, Date): EP 2001272281 011221; WO 2001JP11237 011221

PRIORITY (CC, No, Date): JP 2000396098 001226

DESIGNATED STATES: AT; DE; FR; GB; NL

INTERNATIONAL PATENT CLASS: H04L-009/00; **G06F-012/14** ; **G06F-015/00** ; **G06F-017/60**

ABSTRACT WORD COUNT: 160

NOTE:
Figure number on first page: 0063

LANGUAGE (Publication,Procedural,Application): English; English; Japanese

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200244	1230
SPEC A	(English)	200244	34791
Total word count - document A			36021
Total word count - document B			0
Total word count - documents A + B			36021

...INTERNATIONAL PATENT CLASS: **G06F-012/14** ...
... **G06F-015/00** ...

... **G06F-017/60**

...SPECIFICATION particular user. The document encrypted using the public key can only be decrypted using a **secret key** corresponding to the encryption key used to encrypt that document. The **secret key** is held only by the user who issued the public key, and thus the document encrypted using the public key can be decrypted only by the user having the **secret key** . A representative example of the public key cryptography is that based on the RSA (Rivest...above-described technique thereby allowing the common authentication key to be used as a secure **secret key** and thus allowing authentication to be performed according to the common key cryptography technique. That...

...the device B. Herein, the key Kab is a key that is used as a **secret key** in common by the devices A and B and that is stored in a storage...

the device B decrypts the received data using the key Kab (authentication key) as the **secret key** used in common. More specifically, the decryption of the received data is performed as follows...that can be decrypted only by using a key acquired by processing the EKB and **distributes** the resultant **encrypted key** or content.

First , various entities in the system are described briefly.

Key distribution center (KDC)

A key distribution...produced by the key distribution center (KDC) and issues a public key corresponding to a **secret key** on which a signature is written, for use in verification of the signature.

An EKB...

14/3,K/18 (Item 16 from file: 348)

DIALOG(R)File 348:EUROPEAN PATENTS

01476931

INFORMATION PROCESSING SYSTEM AND METHOD

VERFAHREN UND VORRICHTUNG ZUR INFORMATIONSVERARBEITUNG

SYSTEME ET PROCEDE DE TRAITEMENT D'INFORMATIONS

PATENT ASSIGNEE:

Sony Corporation, (214031), 6-7-35 Kitashinagawa, Shinagawa-ku, Tokyo 141-0001, (JP), (Applicant designated States: all)

INVENTOR:

ASANO, Tomoyuki, c/o SONY CORPORATION, 7-35, KITASHINAGAWA 6-CHOME, SHINAGAWA-KU, Tokyo 141-0001, (JP)

OSAWA, Yoshitomo, c/o SONY CORPORATION, 7-35, KITASHINAGAWA 6-CHOME, SHINAGAWA-KU, Tokyo 141-0001, (JP)

OISHI, Tateo, c/o SONY CORPORATION, 7-35, KITASHINAGAWA 6-CHOME, SHINAGAWA-KU, Tokyo 141-0001, (JP)

ISHIGURO, Ryuji, c/o SONY CORPORATION, 7-35, KITASHINAGAWA 6-CHOME, SHINAGAWA-KU, Tokyo 141-0001, (JP)

TAKI, Ryuta, c/o SONY CORPORATION, 7-35, KITASHINAGAWA 6-CHOME, SHINAGAWA-KU, Tokyo 141-0001, (JP)

LEGAL REPRESENTATIVE:

Pilch, Adam John Michael et al (50481), D. YOUNG & CO., 21 New Fetter Lane, London EC4A 1DA, (GB)

PATENT (CC, No, Kind, Date): EP 1253738 A1 021030 (Basic)
WO 2002052779 020704

APPLICATION (CC, No, Date): EP 2001272279 011221; WO 2001JP11235 011221

PRIORITY (CC, No, Date): JP 2000395105 001226

DESIGNATED STATES: AT; DE; FR; GB; NL

INTERNATIONAL PATENT CLASS: H04L-009/00; **G06F-012/14** ; **G06F-015/00** ; **G06F-017/60**

ABSTRACT WORD COUNT: 149

NOTE:

Figure number on first page: 0047

LANGUAGE (Publication,Procedural,Application): English; English; Japanese

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200244	3050
SPEC A	(English)	200244	36784
Total word count - document A			39834
Total word count - document B			0
Total word count - documents A + B			39834

...INTERNATIONAL PATENT CLASS: **G06F-012/14** ...

... **G06F-015/00** ...

... **G06F-017/60**

...SPECIFICATION particular user. The document encrypted using the public key can only be decrypted using a **secret key** corresponding to the encryption key used to encrypt that document. The **secret key** is held only by the user who issued the public key, and thus the document encrypted using the public key can be decrypted only by the user having the **secret key** . A representative example of the public key cryptography is that based on the RSA (Rivest...above-described technique thereby allowing the common authentication key to be used as a secure **secret key** and thus allowing authentication to be performed according to the common key cryptography technique. That...

...the device B. Herein, the key Kab is a key that is used as a **secret key** in common by the devices A and B and that is stored in a storage... the device B decrypts the received data using the key Kab (authentication key) as the **secret key** used in common. More specifically, the decryption of the received data is performed as follows...that can be decrypted only by using a key acquired by processing the EKB and **distributes** the resultant **encrypted key** or content.
First , various entities in the system are described briefly.

Key distribution center (KDC)
A key distribution...produced by the key distribution center (KDC) and issues a public key corresponding to a **secret key** on which a signature is written, for use in verification of the signature.
An EKB...

14/3,K/19 (Item 17 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01461556
INFORMATION PROCESSING SYSTEM AND METHOD
VERFAHREN UND VORRICHTUNG ZUR INFORMATIONSVERARBEITUNG
SYSTEME ET PROCEDE DE TRAITEMENT D'INFORMATIONS
PATENT ASSIGNEE:
Sony Corporation, (214028), 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001, (JP), (Applicant designated States: all)
INVENTOR:
ASANO, Tomoyuki c/o SONY CORPORATION, 7-35, KITASHINAGAWA 6-CHOME, SHINAGAWA-KU, Tokyo 141-0001, (JP)
OSAWA, Yoshitomo c/o SONY CORPORATION, 7-35, KITASHINAGAWA 6-CHOME, SHINAGAWA-KU, Tokyo 141-0001, (JP)
OISHI, Tateo c/o SONY CORPORATION, 7-35, KITASHINAGAWA 6-CHOME, SHINAGAWA-KU, Tokyo 141-0001, (JP)
ISHIGURO, Ryuji c/o SONY CORPORATION, 7-35, KITASHINAGAWA 6-CHOME, SHINAGAWA-KU, Tokyo 141-0001, (JP)
TAKI, Ryuta c/o SONY CORPORATION, 7-35, KITASHINAGAWA 6-CHOME, SHINAGAWA-KU, Tokyo 141-0001, (JP)
LEGAL REPRESENTATIVE:
Pratt, Richard Wilson et al (46458), D. Young & Co, 21 New Fetter Lane, London EC4A 1DA, (GB)
PATENT (CC, No, Kind, Date): EP 1249962 A1 021016 (Basic)
WO 2002052780 020704
APPLICATION (CC, No, Date): EP 2001272280 011221; WO 2001JP11236 011221
PRIORITY (CC, No, Date): JP 2000395844 001226

DESIGNATED STATES: AT; DE; FR; GB; NL
INTERNATIONAL PATENT CLASS: H04L-009/00; **G06F-012/14** ; **G06F-015/00** ; **G06F-017/60**
ABSTRACT WORD COUNT: 170
NOTE:
Figure number on first page: 0047

LANGUAGE (Publication,Procedural,Application): English; English; Japanese
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200242	5699
SPEC A	(English)	200242	39829
Total word count - document A			45528
Total word count - document B			0
Total word count - documents A + B			45528

...INTERNATIONAL PATENT CLASS: **G06F-012/14** ...
... **G06F-015/00** ...

... **G06F-017/60**

...SPECIFICATION particular user. The document encrypted using the public key can only be decrypted using a **secret key** corresponding to the encryption key used to encrypt that document. The **secret key** is held only by the user who issued the public key, and thus the document encrypted using the public key can be decrypted only by the user having the **secret key** . A representative example of the public key cryptography is that based on the RSA (Rivest...above-described technique thereby allowing the common authentication key to be used as a secure **secret key** and thus allowing authentication to be performed according to the common key cryptography technique. That...

...the device B. Herein, the key Kab is a key that is used as a **secret key** in common by the devices A and B and that is stored in a storage... the device B decrypts the received data using the key Kab (authentication key) as the **secret key** used in common. More specifically, the decryption of the received data is performed as follows...that can be decrypted only by using a key acquired by processing the EKB and **distributes** the resultant **encrypted key** or content.
First , various entities in the system are described briefly.

Key distribution center (KDC)
A key distribution...produced by the key distribution center (KDC) and issues a public key corresponding to a **secret key** on which a signature is written, for use in verification of the signature.
An EKB...

14/3,K/20 (Item 18 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01324429
System and method for distribution and monitoring of copyrighted data
System und Verfahren zur Verteilung und Uberwachung urheberrechtlich geschutzter Daten
Systeme et procede pour la distribution et la surveillance des donnees protegees par un droit d'auteur
PATENT ASSIGNEE:
SONY CORPORATION, (214025), 6-7-35 Kitashinagawa Shinagawa-ku, Tokyo 141,

(JP), (Applicant designated States: all)
INVENTOR:
Hirai, Jun, Intellectual Property Department, Sony Corp., 6-7-35 Kitashinagawa, Shinagawa-ku, Tokyo 141, (JP)
LEGAL REPRESENTATIVE:
Turner, James Arthur et al (74631), D. Young & Co., 21 New Fetter Lane, London EC4A 1DA, (GB)
PATENT (CC, No, Kind, Date): EP 1130500 A2 010905 (Basic)
EP 1130500 A3 040728
EP 1130500 A3 040728
APPLICATION (CC, No, Date): EP 2001300144 010109;
PRIORITY (CC, No, Date): JP 200014195 000120
DESIGNATED STATES: DE; FR; GB
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: **G06F-001/00**
ABSTRACT WORD COUNT: 123
NOTE:
Figure number on first page: 2

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200136	2147
SPEC A	(English)	200136	5953
Total word count - document A			8100
Total word count - document B			0
Total word count - documents A + B			8100

INTERNATIONAL PATENT CLASS: **G06F-001/00**

...SPECIFICATION In this case, the above-described second step can distribute the content via the predetermined **distribution** path with attached authentication information **encrypted** using the encryption **key** issued in the **first** step, making it possible to appropriately prevent the authentication information from being falsified.
The above...the time of encryption and decryption or a public key encryption method in which a **secret key** and a public key are formed in combination may be used. However, in the following...

14/3,K/21 (Item 19 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2005 European Patent Office. All rts. reserv.

01316288
Method of using a mask programmed secret key **to securely configure a field programmable gate array**
Methode zur gesicherten Programmierung eines FPGA mittels eines maskenprogrammierten geheimen Schlussels
Procede de programmabilite d'un circuit integre de type predifuse programmable (FPGA) avec une cle secrete programmee par masque
PATENT ASSIGNEE:
Algotronix Ltd., (1289191), 130/10 Calton Road, Edinburgh EH8 8JQ, (GB), (Applicant designated States: all)
INVENTOR:
Kean, Thomas A, 130/10 Calton Road, Edinburgh, Scotland EH8 8JQ, (GB)
LEGAL REPRESENTATIVE:
O'Connell, David Christopher (62551), Haseltine Lake & Co., Imperial House, 15-19 Kingsway, London WC2B 6UD, (GB)
PATENT (CC, No, Kind, Date): EP 1124330 A2 010816 (Basic)

EP 1124330 A3 010919
APPLICATION (CC, No, Date): EP 2001301150 010209;
PRIORITY (CC, No, Date): GB 2829 000209; US 747759 001221
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: H03K-019/00; G07C-011/00; **G06F-012/14** ; G06K-019/073
ABSTRACT WORD COUNT: 144
NOTE:
Figure number on first page: 5

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Method of using a mask programmed secret key **to securely configure a field programmable gate array**

...INTERNATIONAL PATENT CLASS: **G06F-012/14**

...ABSTRACT using the security key stored in the artwork of the field programmable gate array. The **secret key** consists of a number of bits of key information that are embedded within the photomasks...

...SPECIFICATION using the security key stored in the artwork of the field programmable gate array. The **secret key** consists of a number of bits of key information that are embedded within the photomasks...

...impossible to manufacture cloned products. FPGAs can be manufactured with one of two or more **secret keys** (e.g., key A and key B) embedded in the artwork of the design. After...

...packages are marked identically. A customer who bought FPGAs has no way of telling which **secret key** was present on a particular chip. If the customer was a pirate who had a...

...a problem: since the bitstream can only be decrypted by an FPGA with the matching **secret key** only 50% of the FPGAs that he bought would actually work with his copied bitstream...

...is a method including fabricating a first group of FPGA integrated circuits with a first **secret key** embedded by way of a first mask set. The method includes fabricating a second group of FPGA integrated circuits with a second **secret key** embedded by way of a second mask set. The first group of FPGA integrated circuit...

...between the first group of FPGAs and second group of FPGAs is having a different **secret key** or security key. A first secure bitstream will configure properly user-configurable logic of the...

...integrated circuits.

In an embodiment, the first group of FPGA integrated circuits with the first **secret key** may be assigned to a first geographic area and the second group of FPGA integrated circuits with the second **secret key** may be assigned to a second geographic area. In another embodiment, the first group of FPGA integrated circuits with the first **secret key** are fabricated in a first time period and the second group of FPGA integrated circuits with the second **secret key** are fabricated in a second time period, different from the first time period. The first...

...period. In a further embodiment, the first group of FPGA integrated circuits with the first **secret key** are assigned to a first customer and the second group of FPGA integrated circuits with the second **secret key** are assigned to a second customer.

In an embodiment, only one mask differs between the...

...the first and second group of FPGA integrated circuits in addition to the different embedded **secret keys** .

The method further includes loading an unencrypted bitstream into one of the first group of FPGA integrated circuits to generate a secure bitstream using the first **secret key** . The first and second **secret keys** may be presented on wires of the respective group of FPGA integrated circuits for only a limited duration. The first **secret key** may be embedded by setting an initial state of a selection of memory cells in a device configuration memory of the FPGA integrated circuit. In an embodiment, the first **secret key** is extracted by using a CRC algorithm to compute a checksum of the initial state of the device

...memory of the programmable integrated circuit.
14. The method of claim 1 wherein the first **secret key** is embedded by changes to a relatively large block of logic in the first plurality ...

...using a CRC algorithm.
15. The method of claim 13 further comprising:

extracting the first **secret key** by using a CRC algorithm to compute a checksum of the initial state of the...

...first plurality of programmable integrated circuits to generate a secure bitstream based on the first **secret key** and an on-chip generated random number.
17. The method of claim 1 further comprising...

...first plurality of programmable integrated circuits to generate a secure bitstream based on the first **secret key** and an on-chip generated random number, wherein the secure bitstream includes a message authentication code.
18. A method comprising:
embedding a first **secret key** within the artwork of a programmable integrated circuit;
storing a user-defined second **secret key** within an encrypted programmable integrated circuit bitstream stored in an external nonvolatile memory accessible by the programmable integrated circuit;

decrypting the user-defined second **secret key** using the first **secret key** ; and
setting up a secure network link between the programmable integrated circuit and a server using the user-defined second **secret key** .
19. The method of claim 18 further comprising:
downloading a programmable integrated circuit bitstream using the secure network link;
encrypting the downloaded programmable integrated circuit bitstream using the **first secret key** ; and
storing the **encrypted downloaded** bitstream in the external memory.
20. The method of claim 18 wherein the secure network...

...encrypted downloaded bitstream stored in the external memory.
22. A method comprising:
storing a first **secret key** on a programmable integrated circuit chip;
causing the programmable integrated circuit to calculate a message...

14/3,K/22 (Item 20 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01311508
DEVICE FOR REPRODUCING DATA
DATENWIEDERGABEGERAT
DISPOSITIF DE REPRODUCTION DE DONNEES
PATENT ASSIGNEE:
Sanyo Electric Co., Ltd., (2206455), 5-5, Keihan-Hondori 2-chome,, Moriguchi-shi, Osaka 570-8677, (JP), (Applicant designated States: all)
FUJITSU LIMITED, (211463), 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588, (JP), (Applicant designated States: all)

Hitachi, Ltd., (204145), 6 Kanda Surugadai 4-chome, Chiyoda-ku, Tokyo 101-8010, (JP), (Applicant designated States: all)
Nippon Columbia Co., Ltd., (2395621), 14-14 Akasaka 4-chome, Minato-ku, Tokyo 107-8011, (JP), (Applicant designated States: all)
INVENTOR:
HORI, Yoshihiro, Sanyo Electric Co., Ltd., 5-5, Keihanhondori 2-chome, Moriguchi-shi, Osaka 570-8677, (JP)
HIOKI, Toshiaki, Sanyo Electric Co., Ltd., 5-5, Keihanhondori 2-chome, Moriguchi-shi, Osaka 570-8677, (JP)
KANAMORI, Miwa, Sanyo Electric Co., Ltd., 5-5, Keihanhondori 2-chome, Moriguchi-shi, Osaka 570-8677, (JP)
YOSHIKAWA, Takatoshi, Sanyo Electric Co., Ltd., 5-5, Keihanhondori 2-chome, Moriguchi-shi, Osaka 570-8677, (JP)
TAKEMURA, Hiroshi, Sanyo Electric Co., Ltd., 5-5, Keihanhondori 2-chome, Moriguchi-shi, Osaka 570-8677, (JP)
HASEBE, Takayuki, Fujitsu Limited, 1-1, Kamikodanaka 4-chome, Nakahara-ku , Kawasaki-shi, Kanagawa 211-8588, (JP)
HATAKEYAMA, Takahisa, Fujitsu Limited, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588, (JP)
TONEGAWA, Tadaaki, Hitachi, Ltd., 20-1, Josuihoncho 5-chome, Kodaira-shi, Tokyo 187-8588, (JP)
ANAZAWA, Takeaki Nippon Columbia Co., Ltd., 14-14, Akasaka 4-chome, Minato-ku, Tokyo 107-8011, (JP)
LEGAL REPRESENTATIVE:
Glawe, Delfs, Moll & Partner (100692), Patentanwalte Postfach 26 01 62, 80058 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1237323 A1 020904 (Basic)
WO 2001043339 010614
APPLICATION (CC, No, Date): EP 2000979933 001206; WO 2000JP8615 001206
PRIORITY (CC, No, Date): JP 99347904 991207
DESIGNATED STATES: DE; FR; GB
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: H04L-009/08; H04L-009/32; G09C-001/00; **G06F-017/60**
ABSTRACT WORD COUNT: 109
NOTE:
Figure number on first page: 0004

LANGUAGE (Publication,Procedural,Application): English; English; Japanese
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200236	862
SPEC A	(English)	200236	13834
Total word count - document A			14696
Total word count - document B			0
Total word count - documents A + B			14696

...INTERNATIONAL PATENT CLASS: **G06F-017/60**

...SPECIFICATION is distributed in the encrypted form, on the user side. First, the system requires a **cryptosystem** for **distributing** an **encryption key** in the communication. **Second** , the system requires a cryptosystem for encrypting the data itself to be distributed. Third, the ...keys KPmc(n) and KPp(n), will be referred to as a "class" hereinafter. As **secret keys** common to the content reproducing circuit, the system employs a **secret key** Kcom, which is primarily utilized for obtaining license key Kc and restriction information for the...

...later, as well as an authentication key KPma operated commonly in whole the distribution system. **Secret key** Kcom is a decryption key in the symmetric key cryptosystem, and therefore is held as the encryption key

with public encryption key KPm(1) unique to memory card 110 without being encrypted with **secret key** Kcom. Therefore, step S134 is eliminated. Subsequently to step S132, steps 136a - S148a are executed...

...repeated. Since license key Kc and reproducing circuit restriction control AC2 are not encrypted with **secret key** Kcom, but are encrypted with public encryption key Km(1) unique to memory card 110...

...for that license key Kc and reproducing circuit restriction information AC2 are not encrypted with **secret key** Kcom in the third embodiment. Thus, the operations in the third embodiment are substantially the...

...system according to the first embodiment, can be achieved although the system does not use **secret key** Kcom, which is symmetric to the content reproducing circuit (cellular phone), for performing the encryption...

...the distribution server and the cellular phone do not perform the encryption and decryption using **secret key** Kcom symmetric to the reproducing circuit. The reproducing device may be a device other than...

14/3,K/23 (Item 21 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01311422
DATA DISTRIBUTION SYSTEM AND RECORDER FOR USE THEREIN
DATENVERTEILUNGSVORRICHTUNG UND ZUGEHORIGES AUFZEICHNUNGSGERAT
SYSTEME DE DISTRIBUTION DE DONNEES ET ENREGISTREUR UTILISE AVEC CE SYSTEME
PATENT ASSIGNEE:
Sanyo Electric Co., Ltd., (2206455), 5-5, Keihan-Hondori 2-chome,, Moriguchi-shi, Osaka 570-8677, (JP), (Applicant designated States: all)
PFU LIMITED, (930123), Nu-98-2, Aza-Unoke, Unoke-machi, Kahoku-gun Ishikawa 929-1125, (JP), (Applicant designated States: all)
FUJITSU LIMITED, (211463), 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588, (JP), (Applicant designated States: all)
Hitachi, Ltd., (204145), 6 Kanda Surugadai 4-chome, Chiyoda-ku, Tokyo 101-8010, (JP), (Applicant designated States: all)
Nippon Columbia Co., Ltd., (2395621), 14-14 Akasaka 4-chome, Minato-ku, Tokyo 107-8011, (JP), (Applicant designated States: all)
INVENTOR:
HORI, Yoshihiro, Sanyo Electric Co., Ltd., 5-5, Keihanhondori 2-chome, Moriguchi-shi, Osaka 570-8677, (JP)
HIOKI, Toshiaki, Sanyo Electric Co., Ltd., 5-5, Keihanhondori 2-chome, Moriguchi-shi, Osaka 570-8677, (JP)
KANAMORI, Miwa, Sanyo Electric Co., Ltd., 5-5, Keihanhondori 2-chome, Moriguchi-shi, Osaka 570-8677, (JP)
TAKAHASHI, Masataka, PFU Limited, Aza Unoke Nu98-2, Unoke-machi, Kahoku-gun, Ishikawa 929-1192, (JP)
HASEBE, Takayuki, Fujitsu Limited, 1-1, Kamikodanaka 4-chome, Nakahara-ku , Kawasaki-shi, Kanagawa 211-8588, (JP)
YOSHIOKA, Makoto, Fujitsu Limited, 1-1, Kamikodanak 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588, (JP)
HATAKEYAMA, Takahisa, Fujitsu Limited, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588, (JP)
TONEGAWA, Tadaaki, Semicond. & Integr. Circuits, Hitachi, Ltd., 20-1, Josuihoncho 5-chome, Kodaira-shi, Tokyo 187-8588, (JP)
ANAZAWA, Takeaki, Nippon Columbia Co., Ltd., 14-14,Akasaka 4-chome,

Minato-ku, Tokyo 107-8011, (JP)
LEGAL REPRESENTATIVE:
Glawe. Delfs. Moll (100699), Patentanwalte Postfach 26 01 62, 80058 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1237326 A1 020904 (Basic)
WO 2001043342 010614
APPLICATION (CC, No, Date): EP 2000979088 001205; WO 2000JP8593 001205
PRIORITY (CC, No, Date): JP 99346861 991206
DESIGNATED STATES: DE; FR; GB
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: H04L-009/32; **G06F-012/14** ; G10K-015/02; **G06F-013/00**
ABSTRACT WORD COUNT: 86
NOTE:
Figure number on first page: 0006

LANGUAGE (Publication,Procedural,Application): English; English; Japanese
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200236	4572
SPEC A	(English)	200236	13725
Total word count - document A			18297
Total word count - document B			0
Total word count - documents A + B			18297

...INTERNATIONAL PATENT CLASS: **G06F-012/14** ...

... **G06F-013/00**

...SPECIFICATION of a cellular phone user, a system is initially required to be a system for **distributing** an **e**ncryption key in a communication, **secondly** the exact system encrypting content data to be distributed, and thirdly a configuration implementing decryption...a memory card externally communicates data, encryption keys Ks1-Ks4 are used to keep the **secret** . **Keys** Ks1-Ks4 are symmetric keys generated by server 30, cellular phone 100 or 102, memory...

...number i represents a number provided to distinguish each memory card.
Furthermore, as a common **secret** **key** in a system there exists a **secret** **key** Kcom in a symmetric-key cryptosystem used mainly to obtain license key Kc. **Secret** **key** Kcom is held in both of a distribution server and a cellular phone and used...Ks1 and then transmitted on data bus BS1, and a Kcom hold unit 322 holding **secret** **key** Kcom shared by reproduction circuits.
Data processing unit 310 further includes an encryption unit 324 using **secret** **key** Kcom to encrypt license key Kc and reproduction circuit control information AC2 received from distribution...

...bus BS2 for output.
Cellular phone 100 further includes a Kcom hold unit 1512 holding **secret** **key** Kcom set to be shared by reproduction circuits, a decryption unit 1514 using **secret** **key** Kcom to decrypt (Kc//AC2)Kcom output from decryption unit 1510, and outputting license key...324, which in turn encrypts license key Kc and reproduction circuit control information AC2 with **secret** **key** Kcom shared by reproduction circuit and obtained from Kcom hold unit 322 (step S130).
Encrypted...1) unique to memory card 110 and encrypted data (Kc//AC2)Kcom decryptable with common **secret** **key** Kcom is obtained on data bus BS4 (step S222).
Obtained encrypted data (Kc//AC2)Kcom...

...AC2 are accepted (step S226).
Decryption unit 1514 decrypts encrypted data (Kc//AC2)Kcom with **secret key** Kcom received from Kcom hold circuit 1512 and shared by reproduction circuits to accept license...that of the first embodiment in that the former does not provide encryption decryptable with **secret key** Kcom shared by reproduction circuits.
More specifically the data distribution system of the present embodiment...

...server His different from license server 10 in that the former excludes unit 322 holding **secret key** Kcom shared by reproduction circuits, and encryption unit 324 using **secret key** Kcom. More specifically, in license server 11 license key Kc and reproduction circuit control information...
...100 of the first embodiment in that the former excludes Kcom hold unit 1512 holding **secret key** Kcom shared by reproduction circuits and decryption unit 1514 using **secret key** Kcom.
More specifically, in cellular phone 101, corresponding to the fact that distribution server 31 does not provide encryption using **secret key** Kcom, encryption unit 1510 using session key Ks4 to effect decryption directly provides license key...

...card identical in configuration to the Fig. 6 memory card 110.
Omitting the encryption using **secret key** Kcom shared by reproduction circuits results in a difference in operation in each of distribution...Kc and reproduction circuit control information AC2 obtained at step S128 are not encrypted with **secret key** Kcom and they are encrypted with public encryption key KPm(1) unique. to memory card...

...Kc and AC2 and thus used. Furthermore, step S228 is eliminated as the encryption using **secret key** Kcom is not applied to license key Kc or reproduction control information AC2.
The remaining...

...those shown in Figs. 13 and 14 and thus will not be described.
Thus, if **secret key** Kcom shared by reproduction circuits is not used, a data distribution system can be configured...More specifically, license key Kc and reproduction circuit control information AC2 that are encrypted with **secret key** Kcom in the form of (Kc//AC2)Kcom can be recorded in reproduction information hold...

...CLAIMS second decryption unit (1412) receiving said reproduction information and access restriction information encrypted with said **second** symmetric **key** and said **second** public **encryption key** and **distributed** from said content provision device, for decryption with said second symmetric key,
a third key...content provision device (10) further includes
a fifth key hold unit (322) holding a common **secret key** (Kcom) reproducible in said content reproduction unit, and
a third license data encryption unit (324) encrypting said reproduction information (Kc//AC2, (Kc//AC2)Kcom) with said common **secret key** for output to said first license data encryption unit (326); and
said content reproduction unit further has
a sixth key hold unit (1512) holding said common **secret key** , and
a sixth decryption unit (1514) receiving an output of said fourth decryption unit (1510), decrypting said reproduction information with said common **secret key** held in said sixth key hold unit, and extracting said license key (Kc) for output...provided to record said access restriction information (AC1) therein, said recording device

further comprising:
a **secret key** hold unit (1421) holding a private decryption key (Km(i)) decrypting data encrypted with a...

14/3,K/24 (Item 22 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01308858
RECORDER
REKORDER
ENREGISTREUR
PATENT ASSIGNEE:
Sanyo Electric Co., Ltd., (2206454), 5-5, Keihanhondori 2-chome, Moriguchi-shi, Osaka-fu 570-8677, (JP), (Applicant designated States: all)
FUJITSU LIMITED, (211463), 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588, (JP), (Applicant designated States: all)
Hitachi, Ltd., (204145), 6 Kanda Surugadai 4-chome, Chiyoda-ku, Tokyo 101-8010, (JP), (Applicant designated States: all)
Nippon Columbia Co., Ltd., (2395621), 14-14 Akasaka 4-chome, Minato-ku, Tokyo 107-8011, (JP), (Applicant designated States: all)
INVENTOR:
HORI, Yoshihiro Sanyo Electric Co., Ltd., 5-5, Keihanhondori 2-chome, Moriguchi-shi, Osaka 570-8677, (JP)
HIOKI, Toshiaki Sanyo Electric Co., Ltd., 5-5, Keihanhondori 2-chome, Moriguchi-shi, Osaka 570-8677, (JP)
KANAMORI, Miwa Sanyo Electric Co., Ltd., 5-5, Keihanhondori 2-chome, Moriguchi-shi, Osaka 570-8677, (JP)
KOTANI, Seigou Fujitsu Limited, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588, (JP)
HASEBE, Takayuki Fujitsu Limited, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588, (JP)
HATAKEYAMA, Takahisa Fujitsu Limited, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588, (JP)
TONEGAWA, Tadaaki Semiconductor & Integ. Circuits, Hitachi, Ltd. 20-1, Josuihoncho 5-chome, Kodaira-shi, Tokyo 187-8588, (JP)
ANAZAWA, Takeaki Nippon Columbia Co., Ltd., 14-14, Akasaka 4-chome, Minato-ku, Tokyo 107-8011, (JP)
LEGAL REPRESENTATIVE:
Glawe. Delfs. Moll (100699), Patentanwalte Postfach 26 01 62, 80058 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1248248 A1 021009 (Basic)
WO 2001041104 010607
APPLICATION (CC, No, Date): EP 2000979025 001129; WO 2000JP8457 001129
PRIORITY (CC, No, Date): JP 99340365 991130
DESIGNATED STATES: AT; BE; CH; DE; FR; GB; LI
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: G09C-001/00; H04L-009/08; H04L-009/32; **G06F-017/60**
NOTE:
Figure number on first page: 5
LANGUAGE (Publication,Procedural,Application): English; English; Japanese
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200241	1084
SPEC A	(English)	200241	13533
Total word count - document A			14617
Total word count - document B			0

Total word count - documents A + B 14617

...INTERNATIONAL PATENT CLASS: **G06F-017/60**

...SPECIFICATION in the encrypted form, on the user side. First, the system requires a scheme for **distributing** an **encryption key** in the communication. **Second** , the system requires a scheme for encrypting the data itself to be distributed. Third, the...

...later, as well as an authentication key KPma operated commonly in whole the distribution system. **Secret key** Kcom is a decryption key in the symmetric key cryptosystem, and therefore is held as...data (Kc//AC2)Kcom are recorded in memory 1415 after being re-encrypted with symmetric **secret key** K(1).

Further, the content data can be distributed only after confirming the validities of...holding portion 1451 employed in place of K(1) holding portion 1450 holds predetermined symmetric **secret keys** K(1)x (1 ≤ x ≤ N), which are N in number and are...

14/3,K/25 (Item 23 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01308783
DATA DISTRIBUTION SYSTEM AND RECORDER FOR USE THEREIN
DATENVERTEILUNGSVORRICHTUNG UND ZUGEHORIGES AUFZEICHNUNGSGERAT
SYSTEME DE DISTRIBUTION DE DONNEES ET ENREGISTREUR A UTILISER DANS CE SYSTEME
PATENT ASSIGNEE:
Sanyo Electric Co., Ltd., (2206455), 5-5, Keihan-Hondori 2-chome,, Moriguchi-shi, Osaka 570-8677, (JP), (Applicant designated States: all)
PFU LIMITED, (930123), Nu-98-2, Aza-Unoke, Unoke-machi, Kahoku-gun Ishikawa 929-1125, (JP), (Applicant designated States: all)
FUJITSU LIMITED, (211463), 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588, (JP), (Applicant designated States: all)
Hitachi, Ltd., (204145), 6 Kanda Surugadai 4-chome, Chiyoda-ku, Tokyo 101-8010, (JP), (Applicant designated States: all)
Nippon Columbia Co., Ltd., (2395621), 14-14 Akasaka 4-chome, Minato-ku, Tokyo 107-8011, (JP), (Applicant designated States: all)
INVENTOR:
HORI, Yoshihiro Sanyo Electric Co., Ltd, 5-5, Keihanhondori 2-chome, Moriguchi-shi, Osaka 570-8677, (JP)
HIOKI, Toshiaki Sanyo Electric Co., Ltd, 5-5, Keihanhondori 2-chome, Moriguchi-shi, Osaka 570-8677, (JP)
KANAMORI, Miwa Sanyo Electric Co., Ltd, 5-5, Keihanhondori 2-chome, Moriguchi-shi, Osaka 570-8677, (JP)
YOSHIKAWA, Takatoshi Sanyo Electric Co., Ltd, 5-5, Keihanhondori 2-chome, Moriguchi-shi, Osaka 570-8677, (JP)
TAKEMURA, Hiroshi Sanyo Electric Co., Ltd, 5-5, Keihanhondori 2-chome, Moriguchi-shi, Osaka 570-8677, (JP)
TAKAHASHI, Masataka PFU Limited, Nu98-2, Aza Unoke, Unoke-machi, Kahoku-gun, Ishikawa 929-1192, (JP)
HASEBE, Takayuki Fujitsu Limited, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588, (JP)
FURUTA, Shigeki Fujitsu Limited, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588, (JP)
HATAKEYAMA, Takahisa Fujitsu Limited, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588, (JP)

TONEGAWA, Tadaaki Semiconductor & Integr. Circuits, Hitachi, Ltd 20-1, Josuihoncho 5-chome, Kodaira-shi, Tokyo 187-8588, (JP)
ANAZAWA, Takeaki Nippon Columbia Co., Ltd, 14-14, Akasaka 4-chome, Minato-ku, Tokyo 107-8011, (JP)
LEGAL REPRESENTATIVE:
Glawe. Delfs. Moll (100699), Patentanwalte Postfach 26 01 62, 80058 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1237325 A1 020904 (Basic)
WO 2001041359 010607
APPLICATION (CC, No, Date): EP 2000978048 001201; WO 2000JP8497 001201
PRIORITY (CC, No, Date): JP 99345244 991203
DESIGNATED STATES: DE; FR; GB
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: H04L-009/32; **G06F-012/14** ; G10K-015/02; **G06F-013/00**
ABSTRACT WORD COUNT: 105
NOTE:
Figure number on first page: 0005

LANGUAGE (Publication,Procedural,Application): English; English; Japanese
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200236	5603
SPEC A	(English)	200236	14095
Total word count - document A			19698
Total word count - document B			0
Total word count - documents A + B			19698

...INTERNATIONAL PATENT CLASS: **G06F-012/14** ...
... **G06F-013/00**

...SPECIFICATION of a cellular phone user, a system is initially required to be a system for **distributing** an **encryption key** in a communication, **secondly** the exact system **encrypting** content data to be **distributed** , and thirdly a configuration implementing content data protection for preventing such distributed content data from...a memory card externally communicates data, encryption keys Ks1-Ks4 are used to keep the **secret** . **Keys** Ks1-Ks4 are symmetric keys generated by server 30, cellular phone 100 or 102, memory...

...number i represents a number provided to distinguish each memory card.
Furthermore, as a common **secret key** in a system there exists a **secret key** Kcom in a symmetric-key cryptosystem used mainly to obtain license key Kc. **Secret key** Kcom is held in both of a distribution server and a cellular phone and used to encrypt license key Kc and decrypt and thus obtain the same, respectively.
Note that **secret key** Kcom in the symmetric-key cryptosystem may be replaced by a set of public encryption...

...data bus BS1.
Data processing unit 310 further includes a Kcom hold unit 322 holding **secret key** Kcom shared by reproduction circuits, an encryption unit 324 using **secret key** Kcom to encrypt license key Kc and reproduction circuit control information AC2 received from distribution...bus BS2 for output.
Cellular phone 100 further includes a Kcom hold unit 1512 holding **secret key** Kcom set to be shared by reproduction circuits, a decryption unit 1514 using **secret key** Kcom to decrypt (Kc//AC2)Kcom output from decryption unit 1510, and outputting license key...324, which in turn encrypts license key Kc and reproduction circuit control

for each said recording device,
a fifth encryption unit (1452) using said **secret key** to encrypt data obtained from said third decryption unit (1422) decrypting an output of said...

...decryption key (Km(i)), and
a sixth decryption unit (1454) decrypting data encrypted with said **secret key** ;
said first storage unit (1415) records therein data encrypted by said fifth encryption unit;
said fifth encryption unit encrypts data of said class revocation list (CRL) with said **secret key** ; and
said second storage unit (2415) is arranged external to a security area (TRM) unreadable...

...provision device (10, 11) further includes
a sixth key hold unit (322) holding a common **secret key** (Kcom) reproducible in said content reproduction unit (1550), and
a third license data encryption unit (324) encrypting said first reproduction information with said common **secret key** for output to said first license data encryption unit (326); and
said content reproduction unit (1550) further has
a seventh key hold unit (1512) holding said common **secret key** , and
a seventh decryption unit (1514) receiving an output of said fourth decryption unit (1510), decrypting said first reproduction information with said common **secret key** held in said seventh key hold unit, and extracting said license key (Kc) for output...by said second encryption unit.
37. The recording device of claim 33, further comprising:
a **secret key** hold unit (1450) holding a **secret key** (K(i)) different for each said recording device;
a **secret key** encryption unit (1452) using said **secret key** to effect encryption; and
a **secret key** decryption unit (1454) decrypting data encrypted with said **secret key** , wherein:
said first storage unit (1415) and said second storage unit (2415) are arranged external...

14/3,K/26 (Item 24 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01281923
DATA PROVIDING SYSTEM AND METHOD THEREFOR
DATENVERMITTELNDES SYSTEM UND VERFAHREN HIERZU
SYSTEME ET PROCEDE PERMETTANT DE FOURNIR DES DONNEES
PATENT ASSIGNEE:
Sony Corporation, (214028), 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001, (JP), (Applicant designated States: all)
INVENTOR:
NONAKA, Akira Sony Corporation, 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001, (JP)
EZAKI, Tadashi Sony Corporation, 7-35, Kitashinagawa 6-chome Shinagawa-ku , Tokyo 141-0001, (JP)
LEGAL REPRESENTATIVE:
Korber, Martin, Dipl.-Phys. (88321), Mitscherlich & Partner Patentanwalte Sonnenstrasse 33, 80331 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1132828 A1 010912 (Basic)
WO 200122242 010329

APPLICATION (CC, No, Date): EP 2000961019 000914; WO 2000JP6308 000914
PRIORITY (CC, No, Date): JP 99309721 990917; JP 99309722 990917
DESIGNATED STATES: DE; FR; GB
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: **G06F-015/00** ; G10K-015/02
ABSTRACT WORD COUNT: 111
NOTE:
Figure number on first page: 1

LANGUAGE (Publication,Procedural,Application): English; English; Japanese
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200137	31025
SPEC A	(English)	200137	92868
Total word count - document A			123893
Total word count - document B			0
Total word count - documents A + B			123893

INTERNATIONAL PATENT CLASS: **G06F-015/00** ...

...SPECIFICATION processing apparatus, the content key data and the usage control policy data stored in the **distributed key** file are **decrypted** , and the handling of the **distributed** content data is determined based on the related decrypted usage control policy data.

Also, a...apparatus, and the data processing apparatus by a management apparatus, wherein the management apparatus provides **encrypted** content **key** data and encrypted usage control policy data indicating the handling of the content data to...key file to the data processing apparatus, and the data processing apparatus decrypts the content **key** data and the usage control policy data stored in the distributed key file and determines...of a 30th aspect of the present invention is a data providing system having a **plurality** of data providing apparatuses, a data **distribution** apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein...invention is a data providing system having a plurality of data providing apparatuses, a data **distribution** apparatus, a **plurality** of management apparatuses, a database device, and a data processing apparatus, wherein the data providing...key file received from the management apparatus from the data providing apparatus to the data **distribution** apparatus, and **distributing** a **second** module storing the provided content file and the key file from the data distribution apparatus...

...the distributed second module and determining the handling of the content data stored in the **distributed second** module based on the related decrypted usage control policy data.

Also, a data providing method...content files in the database device, the management apparatuses produce the key files storing the **encrypted** content **key** data and **encrypted** usage control policy data indicating the handling of the content data for the content data...of a 67th aspect of the present invention is a data providing system having a **plurality** of data providing apparatuses, a data **distribution** apparatus, a **plurality** of management apparatuses, a database device, and a data processing apparatus, wherein the data providing...management apparatus, a database device, and a data processing apparatus, wherein the data providing apparatus **encrypts** content data by using content **key** data, produces a content file storing the related encrypted content data, and stores the related...and certifies the legitimacy of the related public key data by attaching a signature by **secret key** data of the EMD service center 102 to the certificate data of the public key...

...content data C using the content key data Kc, and the signature data

...in claim 176, wherein
said data distribution apparatus produces said signature data using its own **secret key** data and
said data processing apparatus verifies the legitimacy of said signature data using public key data corresponding to said **secret key** data.
180.A data providing system as set forth in claim 179, wherein
said data...

14/3,K/27 (Item 25 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01276898
CONTENTS MANAGEMENT SYSTEM, DEVICE, METHOD, AND PROGRAM STORAGE MEDIUM
INHALTSVERWALTUNGSSYSTEM, VORRICHTUNG, VERFAHREN UND PROGRAMMSPEICHERMEDIUM
SYSTEME, DISPOSITIF, PROCEDE ET SUPPORT DE PROGRAMME POUR LA GESTION DE CONTENUS
PATENT ASSIGNEE:
Sony Corporation, (214028), 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001, (JP), (Applicant designated States: all)
INVENTOR:
ISHIBASHI, Yoshihito, Sony Corporation, 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001, (JP)
OHISHI, Tateo, Sony Corporation, 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001, (JP)
MUTO, Akihiro, Sony Corporation, 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001, (JP)
KITAHARA, Jun, Sony Corporation, 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001, (JP)
SHIRAI, Taizou, Sony Corporation, 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001, (JP)
LEGAL REPRESENTATIVE:
DeVile, Jonathan Mark, Dr. et al (91151), D. Young & Co 21 New Fetter Lane, London EC4A 1DA, (GB)
PATENT (CC, No, Kind, Date): EP 1128598 A1 010829 (Basic)
WO 200119017 010315
APPLICATION (CC, No, Date): EP 2000956997 000907; WO 2000JP6089 000907
PRIORITY (CC, No, Date): JP 99253660 990907; JP 99253661 990907; JP 99253662 990907; JP 99253663 990907; JP 99260638 990914; JP 99264082 990917; JP 99265866 990920
DESIGNATED STATES: DE; FR; GB
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: H04L-009/32; **G06F-015/00** ; H04N-005/91; G11B-020/10; G10K-015/04; H04N-007/167
ABSTRACT WORD COUNT: 172
NOTE:
Figure number on first page: 0020

LANGUAGE (Publication,Procedural,Application): English; English; Japanese
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200135	29406
SPEC A	(English)	200135	83907
Total word count - document A			113313
Total word count - document B			0
Total word count - documents A + B			113313

...INTERNATIONAL PATENT CLASS: **G06F-015/00**

...SPECIFICATION not illustrated) to encryption processing section 633 and also holds save key Ksave)) unique to **encryption** processing section 633.

And recording and reproducing apparatus 630 has **encrypted** contents and content **key** Kco)) sent from **first** or second contents sending apparatus 600 or 610 received by sending and receiving section 631... network 5 via a user management section 18. In addition, a public key and a **secret key** of the electronic distribution center 1 as well as a public key and a **secret key** peculiar to equipment maintained by the user are all generated and managed, the public keys...and the handling policy to each of which the electronic signature is added using a **secret key** of the content provider 3 are hereinafter referred to as a content provider secure container...

...a hash function based on data that is desired to be transmitted and using a **secret key** of a public key encryption.

The hash function and the signature will be described. The....

...point on the elliptic curve, r is a digit of G, and Ks)) is a **secret key** (0<Ks))<r). In step S2, a random number u is generated by... data is not tampered, and is the data transmitted from the transmission apparatus holding the **secret key** corresponding to the public key.

In step S11, if the signature data c and d...

...received data is tampered or is not data transmitted from the transmission apparatus holding the **secret key** corresponding to the public key.

Further, although SHA-1 is used as the hash function...

...a public key and the other key that should be kept secret is called a **secret key** .

The elliptic curve encryption method that is representative of the public key encryption method will...

...point on the elliptic curve, r is a digit of G, and Ks)) is a **secret key** (0<Ks))<r). In step S31, the encryption data uG is multiplied by the **secret key** Ks)). In step S32, the X coordinates of (X0)), Y0))) among the encryption data is...

...message, Y1)) is cancelled.

In this way, in the public key encryption method, with the **secret key** being Ks)) and the public keys being G, Ks))G, a key to be used... generation section 45, a signature with respect to the price information is generated using the **secret key** of the service provider 3 held in a tamper resistant memory (not shown) (as in...

...content provider secure container and the price information with an electronic signature added using the **secret key** of he service provider 3 are hereinafter referred to as a service provider secure container...ID, if necessary, or may be unnecessary because it is in the registration information), a **secret key** different for each apparatus, the save key Ksave)), the public key of the electronic distribution... encryption method. In this case, a stored key is not the common key, but the **secret key** peculiar to the extension section 66.)

The content key Kco)) that is encrypted by the...

...certificate (the public key certificate of an apparatus) of the public key corresponding to the **secret key** for each apparatus in the storage module 92, the registration information, the content provider secure...

...module in the encryption processing section 83, the individual ID for specifying an apparatus, the **secret key** that is different for each apparatus, the save key Ksave)), the public key of the...

...charge information is stored as well.) The certificate of the public key corresponding to the **secret key** for each apparatus in the encryption processing section 83, the contents encrypted by the content...

...storage medium exclusively for electronic distribution 120, the individual ID of the recording medium, the **secret key** different for each recording medium, the public key certificate corresponding to the **secret key** (which may be recorded in the external memory 123), the save key Ksave)) to be...and the handling policy and its signature. The signature is data generated by applying the **secret key** Kscp)) of the content provider 2 to a hash value generated by applying the hash...

...key Kd)), a handling policy and signatures. The signature is data generated by applying the **secret key** Kscp)) of the content provider 2 to a hash value generated by applying a hash...key K1)), a handling policy and signatures. The signature is data generated by applying the **secret key** Kscp)) of the content provider 2 to a hash value generated by applying a hash...

...of the content provider 2, and signatures. The signature is data generated by applying the **secret key** Ksca)) of the authentication station to a hash value generated by applying a hash function...

...by the delivery key Kd)), and signatures. The signature is data generated by applying the **secret key** Ksca)) of the authentication station to a hash value generated by applying a hash function...

...by the delivery key Kd)), and signatures. The signature is data generated by applying the **secret key** Ksca)) of the authentication station to a hash value generated by applying a hash function...

...is comprised of price information and signatures. The signature is data generated by applying the **secret key** Kssp)) of the service provider 3 to a hash value generated by applying a hash...

...provider secure container, price information and signatures. The signature is data generated by applying the **secret key** Kssp)) of the service provider 3 to a hash value generated by applying a hash...

...of the service provider 3, and signatures . The signature is data generated by applying the **secret key** Ksca)) of the authentication station to a hash value generated by applying a hash function...of the user apparatus, and the signatures. The signature is data generated by applying the **secret key** Ksca)) of the authentication station to a hash value generated by applying a hash function...bits + 160 bits + 160 bits = 448 bits), and generates signature data A.Sig with a **secret key** held by itself with respect to the data. Further, since scalar times of a base...and BV)) (x coordinates and Y coordinates) , and generates signature data B.Sig with a **secret key** held by itself with respect to the data. Finally, the encryption processing section 65 transfers...

14/3,K/28 (Item 26 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01268075

MEMORY CARD

SPEICHERKARTE

CARTE MEMOIRE

PATENT ASSIGNEE:
FUJITSU LIMITED, (211463), 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588, (JP), (Applicant designated States: all)
Nippon Columbia Co., Ltd., (2395621), 14-14 Akasaka 4-chome, Minato-ku, Tokyo 107-8011, (JP), (Applicant designated States: all)
Hitachi, Ltd., (204145), 6 Kanda Surugadai 4-chome, Chiyoda-ku, Tokyo 101-8010, (JP), (Applicant designated States: all)
Sanyo Electric Co., Ltd., (2206455), 5-5, Keihan-Hondori 2-chome,, Moriguchi-shi, Osaka 570-8677, (JP), (Applicant designated States: all)
INVENTOR:
HATANAKA, Masayuki, Fujitsu Limited, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588, (JP)
KAMADA, Jun, Fujitsu Limited, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588, (JP)
HATAKEYAMA, Takahisa, Fujitsu Limited, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588, (JP)
HASEBE, Takayuki, Fujitsu Limited, 1-1, Kamikodanaka 4-chome, Nakahara-ku , Kawasaki-shi, Kanagawa 211-8588, (JP)
KOTANI, Seigou, Fujitsu Limited, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588, (JP)
FURUTA, Shigeki, Fujitsu Limited, 1-1, Kamikodanaka4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588, (JP)
ANAZAWA, Takeaki, Nippon Columbia Co., Ltd., 14-14,Akasaka 4-chome, Minato-ku, Tokyo, (JP)
TONEGAWA, Tadaaki, Semic./Integ.C. Hitachi Limited, 20-1, Josuihoncho 5-chome, Kodaira-shi, Tokyo 187-8588, (JP)
HIOKI, Toshiaki, Sanyo El. Co., Ltd., 5-5, Keihanhondori 2-chome, Moriguchi-shi, Osaka 570-8677, (JP)
KANAMORI, Miwa, Sanyo El. Co., Ltd., 5-5, Keihanhondori 2-chome, Moriguchi-shi, Osaka 570-8677, (JP)
HORI, Yoshihiro, Sanyo El. Co., Ltd., 5-5, Keihanhondori 2-chome, Moriguchi-shi, Osaka 570-8677, (JP)
LEGAL REPRESENTATIVE:
Glawe. Delfs. Moll (100699), Patentanwalte Postfach 26 01 62, 80058 Munchen, (DE)

PATENT (CC, No, Kind, Date): EP 1209657 A1 020529 (Basic)
WO 200113358 010222
APPLICATION (CC, No, Date): EP 2000950052 000809; WO 2000JP5339 000809
PRIORITY (CC, No, Date): JP 99226406 990810; JP 99349336 991208
DESIGNATED STATES: DE; FR; GB
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: G10K-015/02; **G06F-015/00** ; **G06F-017/60** ; H04L-009/08; H04L-009/32; G06K-019/00; H04H-001/00; H04M-003/42; H04M-003/493; H04M-011/08; G01L-019/00
ABSTRACT WORD COUNT: 110
NOTE:
Figure number on first page: 5

LANGUAGE (Publication,Procedural,Application): English; English; Japanese
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200222	2446
SPEC A	(English)	200222	22741
Total word count - document A			25187
Total word count - document B			0
Total word count - documents A + B			25187

...INTERNATIONAL PATENT CLASS: **G06F-015/00** ...

... **G06F-017/60**

...SPECIFICATION symmetric key encrypted by the first public encryption key, and applies a decryption process. The **first** symmetric **key** is updated and **distributed** for each communication of **encrypted** content data.

The **second** **key** hold unit stores a second public encryption key which is unique to each memory card...Kmedia, Kcard(n), and KPcard(n) are used, as will be described afterwards.

Furthermore, the **secret** **key** to maintain secrecy in data transfer with an external source of the memory card and...respect to each other as to the transfer of a session key and obtaining a **secret** **key** used in transmitting a session key to the other party.

The structure of cellular phone...

...CLAIMS encryption key corresponding to said memory card,

a first decryption processing unit (1404) receiving a **first** symmetric **key** updated and **distributed** for each communication of said **encrypted** content data, and encrypted with said first public encryption key to apply a decryption process...

...claim 3, wherein said second decryption processing unit receives license information data encrypted with said **second** public encryption **key** and further **encrypted** with said **first** symmetric **key** , **distributed** together with said content key, and applies decryption based on said first symmetric key,

wherein...

...claim 7, wherein said second decryption processing unit receives license information data encrypted with said **second** public encryption **key** and further **encrypted** with said **first** symmetric **key** , **distributed** together with said content key, and applies decryption based on said first symmetric key,

wherein...

14/3,K/29 **(Item 27 from file: 348)**
DIALOG(R)File 348:EUROPEAN PATENTS

01171827
Method and system for securely handling information between two information processing devices
Verfahren und Vorrichtung zur gesicherten Datenverarbeitung zwischen zwei Verarbeitungsvorrichtungen
Procede et moyens de gestion securisee d'informations entre deux dispositifs de traitement de donnees
PATENT ASSIGNEE:
International Business Machines Corporation, (200128), New Orchard Road, Armonk, NY 10504, (US), (Applicant designated States: all)
INVENTOR:
Hansmann, Uwe, Birkenstrasse 30/1, 71155 Altdorf, (DE)
Seliger, Frank, In den Kreben 25, 71157 Hildrizhausen, (DE)
LEGAL REPRESENTATIVE:
Teufel, Fritz, Dipl.-Phys. et al (11857), IBM Deutschland

Informationssysteme GmbH, Intellectual Property, Pascalstrasse 100, 70548 Stuttgart, (DE)
PATENT (CC, No, Kind, Date): EP 1022638 A2 000726 (Basic)
EP 1022638 A3 010502
APPLICATION (CC, No, Date): EP 100476 000111;
PRIORITY (CC, No, Date): EP 99100474 990112
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: **G06F-001/00**
ABSTRACT WORD COUNT: 128
NOTE:
Figure number on first page: 1

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200030	1902
SPEC A	(English)	200030	5206
Total word count - document A			7108
Total word count - document B			0
Total word count - documents A + B			7108

INTERNATIONAL PATENT CLASS: **G06F-001/00**

...SPECIFICATION is in the possession of a number of plain-text/cypher-text pairs for a **secret key** . The **secret key** can be obtained by trial and error. The most trivial attack is to find out the **secret key** only through trial and error which is called "Brute force attack". By using a large...the public key prior to transmission of an information and only the owner of the **secret key** is enabled to decrypt again the encrypted message. In particular, that principle for the first...

...n = p x q wherein x = plain text, y = cypher text, e = public key, d = **secret key** , n = public modulus and p, q = secret prime numbers.
For the further details of an...

...has not been altered during transmission. For generating a MAC, a cryptographic algorithm with one **secret key** which is known to both communication partners is utilized. For the calculation of a MAC...the user.
In a preferred embodiment of the invention, the encrypted information unit and the **encrypted first key** are **downloaded** from a central server, e.g. a server interconnected with the Internet, particularly from a...

...CLAIMS least one key.
4. Method according to claim 1 or 2, characterized in that the **decrypted** at least **first key** is **transferred** to the first information processing device (2) and the information unit is decrypted (29) on ...of claims 13 to 19, characterized in that the first device (2) comprises means to **download** the **encrypted** information unit, the **encrypted first key** , and/or the generated signature, and/or the control command, from a central server (4...

14/3,K/30 (Item 28 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01158532

METHOD AND DEVICE FOR PROTECTING DIGITAL DATA BY DOUBLE RE-ENCRYPTION

VERFAHREN UND VORRICHTUNG ZUM SCHUTZ DIGITALER DATEN MITTELS DOPPELTER WIEDERVERSCHLUSSELUNG

PROCEDE ET DISPOSITIF DESTINES A PROTEGER DES DONNEES NUMERIQUES PAR DOUBLE RECRYPTAGE

PATENT ASSIGNEE:
MITSUBISHI CORPORATION, (653514), 6-3 Marunouchi 2-chome, Chiyoda-ku, Tokyo 100-8086, (JP), (Applicant designated States: all)
INVENTOR:
SAITO, Makoto, 2-12-6-104, Kaitori, Tama-Shi, Tokyo 206-0012, (JP)
LEGAL REPRESENTATIVE:
Pfenning, Meinig & Partner GbR (100967), Mozartstrasse 17, 80336 Munchen, (DE)

PATENT (CC, No, Kind, Date): EP 1122910 A1 010808 (Basic)
WO 200022777 000420
APPLICATION (CC, No, Date): EP 99947922 991015; WO 99JP5704 991015
PRIORITY (CC, No, Date): JP 98309418 981015
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: H04L-009/14; G11B-020/10; H04N-007/167; **G06F-017/60**
ABSTRACT WORD COUNT: 189
NOTE:
Figure number on first page: 0008

LANGUAGE (Publication,Procedural,Application): English; English; Japanese
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200132	4006
SPEC A	(English)	200132	13221
Total word count - document A			17227
Total word count - document B			0
Total word count - documents A + B			17227

...INTERNATIONAL PATENT CLASS: **G06F-017/60**

...SPECIFICATION the use request according to a digital signature on an edit program by combining a **secret - key** cryptosystem and a public-key cryptosystem.

Japanese Patent Laid-Open Publication 288940/1996 (USP5,740...audio interface 132 and the printer interface 133 of the copyright management apparatus 140.

A **secret - key** cryptosystem is often used as a cryptosystem for encrypting digital data. The most popular DES (Data Encryption Standard) in the **secret - key** cryptosystems carries out encryption/decryption per 64-bit block unit of data. It is a typical block cipher method in the **secret - key** cryptosystem and has been widely adopted. Using this encryption/decryption per block processing allows to...

...CLAIMS data double re-encrypted by third-changeable-second-changeable keys to be copied or transferred;

decrypting said copied or **transferred** digital data double re-**encrypted** by third-changeable- **second** -changeable **keys** by using said third changeable key to digital data re-encrypted by the second changeable...

...data double re-encrypted by third-changeable-second-changeable keys to

be copied or transferred;
decrypting said copied or **transferred** digital data double re-**encrypted** by third-changeable- **second** -changeable **keys** by using said third changeable key to digital data re-encrypted by the second changeable...

...data double re-encrypted by second-changeable-third-changeable keys to be copied or transferred;
decrypting said copied or **transferred** digital data double re-**encrypted** by **second** -changeable-third-changeable **keys** by using said **second** changeable **key** to digital data re-encrypted by the third changeable key; and
decrypting said digital data...
...data double re-encrypted by second-changeable-third-changeable keys to be copied or transferred;
decrypting said copied or **transferred** digital data double re-**encrypted** by **second** -changeable-third-changeable **keys** by using said **second** changeable **key** to digital data re-encrypted by the third changeable key; and
decrypting said digital data...by third-changeable-second-changeable keys to be copied or transferred;
a third changeable key **decryption** unit for **decrypting** said copied or **transferred** digital data double re- **encrypted** by third-changeable-**second** -changeable **keys** by using said third changeable key to digital data re-encrypted by the second changeable...

...by third-changeable-second-changeable keys to be copied or transferred;
a third changeable key **decryption** unit for **decrypting** said copied or **transferred** digital data double re- **encrypted** by third-changeable-**second** -changeable **keys** by using said third changeable key to digital data re-encrypted by the second changeable changeable-third-changeable keys to be copied or transferred; and
a **second** changeable **key** **decryption** unit for **decrypting** said copied or **transferred** digital data double re- **encrypted** by **second** -changeable-third-changeable **keys** by using said **second** changeable **key** to digital data re-encrypted by the third changeable key, and a third changeable key...

...re-encrypted by second-changeable-third-changeable keys to be copied or transferred; and
a **second** changeable **key** **decryption** unit for **decrypting** said copied or **transferred** digital data double re- **encrypted** by **second** -changeable-third-changeable **keys** by using said **second** changeable **key** to digital data re-encrypted by the third changeable key, and a third changeable key...

14/3,K/31 **(Item 29 from file: 348)**
DIALOG(R)File 348:EUROPEAN PATENTS

01156905
DISTRIBUTING ACCESS TO A DATA ITEM
ZUTEILUNG DES ZUGRIFFS AUF EINEN DATENSATZ
REPARTITION DE L'ACCES A UN ARTICLE DE DONNEES
PATENT ASSIGNEE:
Adobe Systems Incorporated, (1120815), 345 Park Avenue, San Jose, California 95110-2704, (US), (Proprietor designated states: all)
INVENTOR:
KAWELL, Leonard, M., Jr., , Concord, MA, (US)

DIAZ, Thomas, R., , Lexington, MA, (US)
HEINEN, Mary, Ellen, , Concord, MA, (US)
HEINEN, Rodger, J., Jr., , Islesboro, ME, (US)
LEGAL REPRESENTATIVE:
McLeish, Nicholas Alistair Maxwell et al (74621), Boult Wade Tennant
Verulam Gardens 70 Gray's Inn Road, London WC1X 8BT, (GB)
PATENT (CC, No, Kind, Date): EP 1125182 A1 010822 (Basic)
EP 1125182 B1 030102
WO 2000020950 000413
APPLICATION (CC, No, Date): EP 99954794 991007; WO 99US23474 991007
PRIORITY (CC, No, Date): US 167888 981007
DESIGNATED STATES (Pub A): AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE;
IT; LI; LU; MC; NL; PT; SE; (Pub B): DE; GB
INTERNATIONAL PATENT CLASS: **G06F-001/00**
NOTE:
No A-document published by EPO
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	200301	1230
CLAIMS B	(German)	200301	621
CLAIMS B	(French)	200301	742
SPEC B	(English)	200301	8607
Total word count - document A			0
Total word count - document B			11200
Total word count - documents A + B			11200

INTERNATIONAL PATENT CLASS: **G06F-001/00**

...SPECIFICATION to the data item. At least one of the transfers of permission may include the **transfer** of a **first encryption key** , and the method may include using a **second encryption key** to **encrypt** the **first encryption key** prior to **transfer** . The **first encryption key** may include a **secret key** and the second encryption key may include one of the keys in a public/private...each of the sender computers and recipient computers may rely on encryption devices known as **secret keys** and public/private key sets, and may include a highly secure mechanism, which may handle...

...more of the keys or key sets, or encrypted or unencrypted data, or both. A **secret key** (also known as a symmetric key) is a string of data (e.g., 40 bits...

...in a way that allows the other data to be de-encrypted using the same **secret key** . A public/private key set includes two strings of data (e.g., 1024 bits each...

...Security Dynamics, Inc., 1982.
A conventional general-purpose computer can be used to generate the **secret key** and the public/private key set, which can be stored in conventional computer files, as...implement a public/private key encryptor 56, a public/private key de-encryptor 58, a **secret key** encryptor 60, and a **secret key** de-encryptor 62. A permission data bank 64, a public key 66, a private key...

...known as Java.
In a specific embodiment, only the publisher computer is provided with a **secret key** encryptor (e.g., because the other computers are not originators of encrypted data items) and only the end-user computer is provided with the **secret key** de-encryptor (e.g., because the other

computers do not display or otherwise make significant...

...Figs. 8-14 illustrate a detailed example 72 of the usage permission transfer procedure. A **secret key** 74 (e.g., a randomly-generated 40-bit number) is used to encrypt book data 76 to produce **secret key** encrypted book data 78 (step 2010), which is stored at a sender computer (step 2020). (In a specific embodiment, the **secret key** is also appended to the **secret key** encrypted book data.)

The encrypted digest and the recipient computer's unique public key are ...

...response can be matched to the request at the recipient computer.) At the sender computer, **secret key** encrypted book data and a **secret key** and voucher corresponding to the request are selected (step 2130), and the recipient's unique public key is used to produce a public key encrypted **secret key** and voucher 94 (step 2140), which is transmitted along with the **secret key** encrypted book data to the recipient computer from the sender computer (steps 2150, 2160).

At...

...recipient computer (Fig. 11), the recipient's unique private key is used to produce a **secret key** and voucher 98 (step 2180), and the **secret key** is used to produce unencrypted book data 100 from the **secret key** encrypted book data (step 2190).

At this point, the unencrypted book data may be displayed...book retailer). If the permission is lent or leased, the procedure also specifies that the **secret key** is associated with matching expiration times 102S and 102R (e.g., each corresponding to a two-week period) at the sender and recipient computers, respectively, so that the **secret key** cannot be used (and therefore the data item cannot be used) at the sender computer...

...In a case of giving or selling, the recipient computer is entitled to retain the **secret key** indefinitely, and to serve as a sender computer in a subsequent transaction. If at the...

...one end-user computer (e.g., itself) to gain access to the data item, the **secret key** is erased at the sender computer after the recipient computer is provided with the **secret key** .

In a case of leasing or selling, the permission may be provided in exchange for...

...In at least some cases, it is advantageous if at least the audit file, the **secret key** , the public/private key set, the permission data bank, the group private key, and the...

...the smartcard computer (i.e., are never presented at the connection circuitry), and if the **secret keys** are never transmitted in unencrypted form. The encrypted data item may be stored separately from ...known as Java.

In a specific embodiment, only the publisher computer is provided with a **secret key** encryptor (e.g., because the other computers are not originators of encrypted data items) and only the end-user computer is provided with the **secret key** de-encryptor (e.g., because the other computers do not display or otherwise make significant...

...Figs. 8-14 illustrate a detailed example 72 of the usage permission transfer procedure. A **secret key** 74 (e.g., a randomly-generated 40-bit number) is used to encrypt book data 76 to produce **secret key** encrypted book data 78 (step 2010), which is stored at a sender computer

secret key and the second encryption key includes one of the keys in a public/private key...

14/3,K/32 (Item 30 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01030324
MOBILE ELECTRONIC COMMERCE SYSTEM
MOBILES ELEKTRONISCHES HANDELSSYSTEM
SYSTEME DE COMMERCE ELECTRONIQUE MOBILE
PATENT ASSIGNEE:
MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD, (216884), 1006, Oaza-Kadoma, Kadoma-shi, Osaka 571-0000, (JP), (Applicant designated States: all)
INVENTOR:
TAKAYAMA, Hisashi, 5-6-12-104, Matsubara, Setagaya-ku, Tokyo 156-0043, (JP)
LEGAL REPRESENTATIVE:
Grunecker, Kinkeldey, Stockmair & Schwanhausser Anwaltssozietat (100721), Maximilianstrasse 58, 80538 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 950968 A1 991020 (Basic)
WO 9909502 990225
APPLICATION (CC, No, Date): EP 98937807 980813; WO 98JP3608 980813
PRIORITY (CC, No, Date): JP 97230564 970813
DESIGNATED STATES: DE; FR; GB
RELATED DIVISIONAL NUMBER(S) - PN (AN):
(EP 2004015278)
INTERNATIONAL PATENT CLASS: **G06F-017/60**
ABSTRACT WORD COUNT: 150
NOTE:
Figure number on first page: 1

LANGUAGE (Publication,Procedural,Application): English; English; Japanese
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	9942	17239
SPEC A	(English)	9942	160346
Total word count - document A			177585
Total word count - document B			0
Total word count - documents A + B			177585

INTERNATIONAL PATENT CLASS: **G06F-017/60**

...SPECIFICATION and then transmits the ticket transfer offer message,via the wireless communication means to the **second** electronic wallet; the **second** electronic wallet, upon receiving the ticket **transfer** offer message, generates a ticket **transfer** offer response message indicating the contents of the ticket transfer offer message are acceptable, and... 108, and between the service system 110 and the telephone card issuing system 109. A **secret key** and a public key are employed for encrypting the information, and the encrypted information is...1511, the audio codec 1512 and the channel codec.

The cryptographic processor 1505 includes a **secret key** encryption and decryption function and a public key encryption and decryption function. The cryptographic processor...data encryption key register (CRYPT) 1613 in which is stored an encryption key for the **secret key** cryptography method that is employed for encryption and decryption of audio data. When the audio...

14/3,K/33 (Item 31 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00968151
Data content dealing system
System zum Behandeln von Dateninhalten
Systeme de transaction de contenu de donnees
PATENT ASSIGNEE:
MITSUBISHI CORPORATION, (653510), 6-3, Marunouchi 2-chome, Chiyoda-ku, Tokyo 100-0005, (JP), (Applicant designated States: all)
INVENTOR:
Saito, Makoto, 2-12-6-104 Kaitori, Tama-shi, (JP)
LEGAL REPRESENTATIVE:
Pfenning, Meinig & Partner (100961), Mozartstrasse 17, 80336 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 878753 A2 981118 (Basic)
EP 878753 A3 010912
APPLICATION (CC, No, Date): EP 98107668 980428;
PRIORITY (CC, No, Date): JP 97126357 970430
DESIGNATED STATES: BE; CH; DE; ES; FR; GB; IT; LI; NL
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: **G06F-001/00**
ABSTRACT WORD COUNT: 142
NOTE:
Figure number on first page: 1

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	9847	963
SPEC A	(English)	9847	13156
Total word count - document A			14119
Total word count - document B			0
Total word count - documents A + B			14119

INTERNATIONAL PATENT CLASS: **G06F-001/00**

...SPECIFICATION to the key management center. On receiving the copyright management program, the key management center **transfers** the **first crypt key** corresponding to the specific usage and a **second crypt key** K2 together with the **copyright** management program to the first user via a communication network. On receiving the first crypt...basic encryption-related technique used in the present invention will be described below.

--Crypt key--
Secret - key system is also called "common key system" because the same key is used for encryption...

...and because it is necessary to keep the key in secret, it is also called " **secret - key** system". Typical examples of encryption algorithm using **secret - key** are: DES (Data Encryption Standard) ...of NTT, and MISTY system of Mitsubishi Electric Corp. In the embodiments described below, the **secret - key** is referred as "Ks".
In contrast, the public-key system is a cryptosystem using a...

...to encrypt data content, a plain text material M to a cryptogram Cmks using a **secret - key** Ks is expressed as:

Cmks = E (M, Ks).

The operation to decrypt the cryptogram Cmks...the second public-key Kb2 that are prepared by a first user, and a first **secret - key** Ks1 and a second **secret - key** Ks2 prepared by the database. The database uses the first **secret - key** Ks1 to encrypt data content M:

Cmks1 = E (M, Ks1)
and further encrypts the first **secret - key** Ks1 by the first public-key Kb1:

Cks1kb1 = E (Ks1, Kb1)

and the second **secret - key** Ks2 by the second public-key Kb2:

Cks2kb2 = E (Ks2, Kb2).

The database then transmits these encrypted data content Cmks1 and the first and the second **secret - keys** Cks1kb1 and Ck2kb2 to the first user.

The first user decrypts the encrypted first **secret - key** Cks1kb1 using the first private-key Kv1:

Ks1 = D (Kv1, Cks1kb1),

and decrypts the encrypted data content Cmks1 by the decrypted first **secret - key** Ks1:

M = D (Ks1, Cmks1)
and uses it. The user decrypts encrypted second **secret - key** Cks2kb2 by the second private-key Kv2:

Ks2 = D (Kv2, Cks2kb2),

which is subsequently used...The original data contents M1, M2 and M3 are encrypted using each of the second **secret - keys** Ks21, Ks22, Ks23 supplied with each of data contents M1, M2 and M3 when used...

...M5 and M6, of original data contents are also encrypted using each of the second **secret - keys** Ks21, Ks22, Ks23 supplied with each of the original data contents when used for operations...

...content parts Cm4ks21, Cm5ks22 and Cm6ks23, and the edit program Pe, second user requests second **secret - keys** Ks21, Ks22, Ks23 for decryption of the encrypted original data content parts Cm4ks21, Cm5ks22 and...

...user is a valid user to use the original data content to which the second **secret - keys** Ks21, Ks22, Ks23 correspond. If the first user is the valid user, the center transmits the second **secret - keys** Ks21, Ks22, Ks23 to second user. Otherwise, it does not transmit the second **secret - keys** Ks21, Ks22, Ks23 to the second user.

The digital signature Spe presented to the copyright...

...content.

(Embodiment 2)

Embodiment 2 is described referring to Figure 3. This embodiment uses first **secret - key** Ks1, second **secret - key** Ks2, third **secret - key**

...scenario market management center to advertise and auction said editing scenario and to change the **secret - key** for said editing scenario from the data content editor's **secret - key** into the scenario seller's **secret - key** ; and
- a database comprising
- the original data content as a data object; and
- said edited...

...stored in said database,
- encrypting the editing scenario of said edited data content by his **secret - key** , depositing the encrypted editing scenario in said database and depositing said **secret - key** in said key management center by said data content editor
- auctioning and transferring of his **secret - key** for said editing scenario to said key management center for said editing scenario seller wishing...

...scenario by an editing scenario market management center; and.
- changing the data content editor's **secret - key** into the editing scenario's seller's key by said editing scenario dealing management center...

14/3,K/34 (Item 32 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00954013
Data management system
Datenverwaltungssystem
Systeme de gestion de donnees
PATENT ASSIGNEE:
MITSUBISHI CORPORATION, (653510), 6-3, Marunouchi 2-chome, Chiyoda-ku, Tokyo 100-0005, (JP), (Applicant designated States: all)
INVENTOR:
Saito, Makoto, 2-12-6-104, Kaitori, Tama-shi, (JP)
LEGAL REPRESENTATIVE:
Pfenning, Meinig & Partner (100961), Mozartstrasse 17, 80336 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 864959 A2 980916 (Basic)
EP 864959 A3 010919
APPLICATION (CC, No, Date): EP 98104490 980312;
PRIORITY (CC, No, Date): JP 9776555 970312
DESIGNATED STATES: BE; CH; DE; ES; FR; GB; IT; LI; NL
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: **G06F-001/00**
ABSTRACT WORD COUNT: 238
NOTE:
Figure number on first page: 1

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	9838	2965
SPEC A	(English)	9838	9634
Total word count - document A			12599
Total word count - document B			0
Total word count - documents A + B			12599

INTERNATIONAL PATENT CLASS: **G06F-001/00**

...SPECIFICATION persons other than the participants of the conference are protected by the cryptosystem using a **secret - key** .

However, since the conference content obtained by the participants themselves are decrypted, in the case...

...public.

The digital cash system which has been proposed so far is based on a **secret - key** cryptosystem. The encrypted digital cash data content is transferred from a bank account or a...

...basic encryption-related technique used in the present invention will be described below.

--Crypt key--

Secret - key system is also called "common key system" because the same key is used for encryption...

...and because it is necessary to keep the key in secret, it is also called " **secret - key** system". Typical examples of encryption algorithm using **secret - key** are: DES (Data Encryption Standard) system of National Bureau of Standards, FEAL (Fast Encryption Algorithm...

...of NTT, and MISTY system of Mitsubishi Electric Corp. In the embodiments described below, the **secret - key** is referred as "Ks".

In contrast, the public-key system is a cryptosystem using a...

...to encrypt data content, a plain text material M to a cryptogram Cks using a **secret - key** Ks is expressed as: The operation to decrypt the cryptogram Cks to the plain text data content M using a **secret - key** Ks is expressed as: Also, the operation to encrypt the plain text ...key escrow system or a key recovery system is used in practical application.

Further, the **secret - key** can be used as user data and the **secret - key** is encrypted using the public-key of the data center and this is entered as...

...this using the private-key of the data center when necessary and by confirming the **secret - key** , it is possible to achieve a key escrow system or a key recovery system in...

...and a public-key Kb1 of the first user, and requests the distribution of a **secret - key** Ks1 for decryption and a **secret - key** Ks2 for re-encryption.

As the user data, a user ID, a user E-mail address or a **secret - key** generated at the user's request for **secret - key** can be used. Further, random number ...hash algorithm, can be used as the user data.

(3) The key center generates the **secret - keys** Ks1 and Ks2 and stores them together with the data content name Tm0, the first user data I1 and the first user public-key Kb1, and the **secret - keys** Ks1 and Ks2 are encrypted using the first user public-key Kb1: and the encrypted **secret - keys** Cks1kb1 and Cks2kb1 are distributed to the first user.

(4) The first user U1 decrypts the distributed encrypted **secret - keys** Cks1kb1 and Cks2kb1 using the first user private-key Kv1:

The decrypted **secret - keys** Ks1 and Ks2 are stored in the device. The user is not the owner of the **secret - keys** Ks1 and ks2, but the key center or the data center is the owner. Because there may be possibility of improper use of the **secret - keys** if the management of the **secret - keys** is made by the user, the **secret - keys** Ks1 and Ks2 are automatically stored in IC card, PCMCIA card, insert board or software...

...user's control.

Here, the fee to use the data content M0 is charged.

14/3,K/35 (Item 33 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00912775
Secure data management system
Gesichertes Datenverwaltungssystem
Systeme securise de gestion de donnees
PATENT ASSIGNEE:
MITSUBISHI CORPORATION, (653510), 6-3, Marunouchi 2-chome, Chiyoda-ku, Tokyo 100-0005, (JP), (Proprietor designated states: all)
INVENTOR:
Saito, Makoto, 2-12-6-104 Kaitori, Tama-shi, Tokyo, (JP)
LEGAL REPRESENTATIVE:
Heselberger, Johannes (90541), Patent- und Rechtsanwalte Bardehle . Pagenberg . Dost . Altenburg . Geissler Galileiplatz 1, 81679 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 833241 A2 980401 (Basic)
EP 833241 A3 990818
EP 833241 B1 050511
APPLICATION (CC, No, Date): EP 97116728 970925;
PRIORITY (CC, No, Date): JP 96277125 960927
DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FI; FR; GB; IT; LI; LU; NL; PT; SE
EXTENDED DESIGNATED STATES: AL; LT; LV; RO; SI
INTERNATIONAL PATENT CLASS: **G06F-001/00**
ABSTRACT WORD COUNT: 237
NOTE:
Figure number on first page: 3A 3B 3C 3D

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	199814	2249
CLAIMS B	(English)	200519	875
CLAIMS B	(German)	200519	833
CLAIMS B	(French)	200519	1086
SPEC A	(English)	199814	13906
SPEC B	(English)	200519	14116
Total word count - document A			16158
Total word count - document B			16910
Total word count - documents A + B			33068

INTERNATIONAL PATENT CLASS: **G06F-001/00**

...SPECIFICATION who use the network. The data management center certifies public-key of network users, distributes **secret - key** for data encryption corresponding to presentation of a user label, and identifies data utilization status by the request of the **secret - key** . The data is stored and transferred after having been encrypted using the **secret - key** , and the data is to be stored and transferred encrypted using a **secret - key** different from the **secret - key** for the data which has been transferred. An original data label is added to an...

...label and the data relating to editing. A user label is used to request the **secret - key** , but electronic fingerprinting of the user label may be used instead.
The second aspect of...

...network, data which is transferred from a maker to a user is encrypted by a **secret - key** for encryption, and data which is transferred from the user to the maker is encrypted by a **secret - key** for re-encryption.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1A to Fig. 1D each represents...

...In this system, a set of public-key & private-key of each user and a **secret - key** different for each step of the use of the copyrighted data are used. Among these...

...be given on a key system and a digital signature system used in the invention.

Secret - key system is also called "common key system" because the same key is used for encryption...

...decryption. Because it is necessary to keep the key in secret, it is also called " **secret - key** system". Typical examples of encryption algorithm using **secret - key** are: DES (Data Encryption Standard) system of National Bureau of Standards, FEAL (Fast Encryption Algorithm...

...of NTT, and MISTY system of Mitsubishi Electric Corp. In the embodiments described below, the **secret - key** is referred as "Ks".

In contrast, the public-key system is a cryptosystem using a...carried out as explained in the third embodiment. In the system of the present embodiment, **secret - key** and public-key & private-key are used. Therefore, an entity to manage public-key and an entity to generate **secret - key** may be linked to or included in the data management center.

(1) An original author...

...original copyright label L0 and requests the data management center Cd to distribute an original **secret - key** Ks0. The original author may transfer or deposit the original copyrighted data to an information...

...the original author. It is also possible that the original author A stores the origins **secret - key** Ks0 and encrypts the original copyrighted data M0 without depending on the data management center Cd, while the original **secret - key** Ks0 must be stored at the data management center Cd to utilize the original copyrighted data M0 by the user (data user).

(2) When the distribution of the original **secret - key** Ks0 is requested, the data management center Cd encrypts the original **secret - key** Ks0 corresponding to the original copyright label L0 using a public-key Kba of the original author A: and distributes the encrypted original **secret - key** Cks0kba together with the original copyright label L0 to the original author A.

The **secret - key** is hereafter, encrypted by a public-key of a distributed destination in order to be...

...this electronic fingerprint is transferred together with the copyrighted data.

(3) When the encrypted original **secret - key** Cks0kba is distributed, the original author A decrypts the encrypted original **secret - key** Cks0kba using the private-key Kva of the original author A: encrypts the original copyrighted data M0 using the decrypted original **secret - key** Ks0: and transfers the encrypted original copyrighted data Cm0ks0, the original copyright label L0 and...

agency;
Decryption of encrypted **secret - key** for re-encryption by using private-key of said user, decryption of encrypted electronic commerce data by using decrypted **secret - key** for re-encryption, making of order sheet by entering order content into decrypted electronic commerce data, encrypting said order sheet by using **secret - key** for re-encryption, and transfer of encrypted order sheet to said agency by said user;
Decryption of said encrypted order sheet by using said **secret - key** for re-encryption, encryption of the decrypted order sheet by using public-key of said...

14/3,K/36 (Item 34 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00907546
Method and apparatus for cryptographically protecting data
Verfahren und Vorrichtung zum kryptographischen Schutz von Daten
Methode et dispositif pour la protection cryptographique de donnees
PATENT ASSIGNEE:
AT&T Corp., (589370), 32 Avenue of the Americas, New York, NY 10013-2412, (US), (applicant designated states:
AT;BE;CH;DE;DK;ES;FI;FR;GB;GR;IE;IT;LI;LU;MC;NL;PT;SE)
INVENTOR:
Fraser, Alexander Gibson, 62 Carriage House Road, Bernardsville, New Jersey 07924, (US)
Odlyzko, Andrew M., 796 Mountain Avenue, Berkeley Heights, New Jersey 07922, (US)
Keshav, Srinivasan, 199 Christopher Lane, Ithaca New York 14850, (US)
LEGAL REPRESENTATIVE:
Suckling, Andrew Michael (77593), Marks & Clerk 4220 Nash Court Oxford Business Park South, Oxford OX4 2RU, (GB)
PATENT (CC, No, Kind, Date): EP 828210 A2 980311 (Basic)
EP 828210 A3 990414
APPLICATION (CC, No, Date): EP 97306098 970811;
PRIORITY (CC, No, Date): US 707691 960904
DESIGNATED STATES: DE; FR; GB
INTERNATIONAL PATENT CLASS: **G06F-001/00**
ABSTRACT WORD COUNT: 69

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	9811	2166
SPEC A	(English)	9811	3126
Total word count - document A			5292
Total word count - document B			0
Total word count - documents A + B			5292

INTERNATIONAL PATENT CLASS: **G06F-001/00**

...SPECIFICATION interaction necessary with a registration authority. Since each digital asset is encrypted with a special **secret key** (lambda)T)) for that specific asset, and can be played or used only when the...

...such as, for example, software, music, art, books, videos, etc., is encrypted with its own **secret key** so that the asset is locked. To simplify the description of the present invention, the...

...of the present invention can be broadcast freely because it cannot be played unless the **secret key** for the piece is known. The music piece can be obtained from any medium, such...

...decryption, and stream decryption in a well-known manner. Personality module PM also stores a **secret key** p and a public key PuA from a certification authority in a memory or database...

...a plurality of personality modules. Each personality module owned by a user has the same **secret key** (rho). Thus, the user can simultaneously play a particular piece of music on as many...common trusted authority. After successful authentication, the certification module enables the vendor to send the **secret key** to the buyer's personality module for the purchased piece of music so that the music can be played. The transmission of the **secret key** for the purchased music is encrypted so there is no need for physical contact between...

...public key Pu<e>, a private key Pr<e> and a **secret key** <(epsilon)>. Plaintext p encrypted by a key k is denoted as k(p...

...a certifying authority A has a public key PuA, a private key PrA and a **secret key** (alpha). A certifying authority certifies the authenticity of keys used by music publishing labels and...

...denoted as entity L, has a public key PuL, a private key PrL and a **secret key** (lambda). Players, denoted at P, are hardware devices (Figure 1) that are manufactured by manufacturer M. Each player plays music and contains a personality module PM that has a **secret key** (rho). Vendors, denoted as V, distribute music, and generally speaking, have a certification module CM...

...denoted as T, represents a piece of music being sold. Each title has an associated **secret key** (lambda)T)) determined by the music publishing label L.

Consider the example of a music...

...publishing label L.

At step 302, the music publishing label L stores the label's **secret key** (lambda), the label's private key PrL, the certification authority's public key PuA, a...key encryption and decryption.

Publishing label L encrypts the piece of music T using a **secret key** for that particular piece of music (lambda)T)) to obtain (lambda)T))(T). Label L also encrypts the **secret key** (lambda)T)) using **secret key** (lambda) to obtain (lambda)((lambda)T))). At step 303, publishing label L sends the encrypted...

...304 by a manufacturer M by encrypting the publicly-known character string X using the **secret key** (rho) for the personality module to obtain (rho)(X). Manufacturer M then provides (rho)(X...

...are provided to manufacturer M.

At step 305, manufacturer M stores the personality module's **secret key** (rho), the certification PrA((rho)X), the certification authority's public key PuA and a...

...the publishing label's public key PuL. Personality module PM uses PuL to encrypt PM **secret key** (rho) and certificate PrA(pX), which are both transferred to certification module CM.

At step 308, certification module CM uses the publishing label's **secret key** PrL to decrypt the personality module's **secret key**

encrypted using the first **secret key** (rho).

36. The personality module according to claim 35, wherein the transceiver receives the encrypted second **secret key** (rho)((lambda)T))) and the selected information, and

wherein the database decrypts the second **secret key** (lambda)T)) using the first **secret key** (rho) stored in the database, and decrypts the encrypted selected information using the second **secret key** (lambda)T)) decrypted by the personality module.

37. The personality module according to claim 36...

...an encrypted first public key PrA(PuL), a second public key PuA, an encrypted first **secret key** (lambda)((lambda)T))), a second **secret key** (lambda), a first private key PrL and first certification information, the first public key PuL being encrypted using a second private key PrA, and the first **secret key** (lambda)T)) being encrypted using the second **secret key** (lambda); and

a transceiver receiving second certification information,

the certification module verifying the second certification...

...claim 40, wherein the second certification information received by the transceiver includes an encrypted third **secret key** PuL((rho)) and the first ...information encrypted with the first public key, the second private key PrA and the third **secret key** (rho).

42. The certification module according to claim 41, wherein the certification module decrypts the encrypted third **secret key** PuL((rho)) using the second private key PrL stored in the database, decrypts the encrypted...

...private key PrL stored in the database, the second public key PuA and the third **secret key** (rho) decrypted by the certification module, and

wherein the certification module enables transmission of the...

...certification module according to claim 42, wherein the selected information is encrypted with the first **secret key** (lambda)T))(T), and

wherein, when the second certification information matches the first certification information, the certification module encrypts the first **secret key** (lambda)T))(T) using the third **secret key** (rho) decrypted by the certification module, and the encrypted first **secret key** (rho)((lambda)T))) is transmitted by the transceiver.

44. The certification module according to claim...

...wherein the second certification information is the first certification information X encrypted using the third **secret key** (rho), and further encrypted by the first private key PrA.

45. The certification module according...

14/3,K/37 (Item 35 from file: 348)

DIALOG(R)File 348:EUROPEAN PATENTS

00760259

Apparatus for data copyright management system

Gerat fur Dateiurheberrechte-Verwaltungssystem

Appareil pour systeme de gestion de droits d'auteur de donnees

PATENT ASSIGNEE:
MITSUBISHI CORPORATION, (653510), 6-3, Marunouchi 2-chome, Chiyoda-ku, Tokyo 100-0005, (JP), (Proprietor designated states: all)
INVENTOR:
Saito, Makoto, 2-12-6-104, Kaitori, Tama-shi, Tokyo, (JP)
Momiki, Shunichi, 4-20-66, Kumegawa-cho, Higashimur-ayama-shi, Tokyo, (JP)
LEGAL REPRESENTATIVE:
Pfenning, Meinig & Partner (100961), Mozartstrasse 17, 80336 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 715241 A2 960605 (Basic)
EP 715241 A3 990203
EP 715241 B1 040114
APPLICATION (CC, No, Date): EP 95116615 951021;
PRIORITY (CC, No, Date): JP 94264200 941027; JP 94299835 941202
DESIGNATED STATES: DE; FR; GB
INTERNATIONAL PATENT CLASS: **G06F-001/00** ; H04N-007/167
ABSTRACT WORD COUNT: 375
NOTE:
Figure number on first page: 3

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPAB96	539
CLAIMS B	(English)	200403	456
CLAIMS B	(German)	200403	421
CLAIMS B	(French)	200403	520
SPEC A	(English)	EPAB96	15016
SPEC B	(English)	200403	15037
Total word count - document A			15559
Total word count - document B			16434
Total word count - documents A + B			31993

INTERNATIONAL PATENT CLASS: **G06F-001/00** ...

...SPECIFICATION is described below, general description is made for cryptography at first.
The cryptography includes a **secret - key** cryptosystem and a public-key cryptosystem.
The **secret - key** cryptosystem is a cryptosystem using the same crypt key for encryption and decryption. While this cryptosystem requires only a short time for encryption or decryption, the **secret - key** is found, and thus, the cryption may be cryptanalized.
The public-key cryptosystem is a...

...M is expressed as (Formula omitted)
The cryptosystem used for the present invention uses a **secret - key** cryptosystem in which the same **secret - key** Ks is used for encryption and decryption, and a public-key cryptosystem in which a...

...supplied in accordance with a request from the primary user 4.
This system rises the **secret - key** cryptosystem and the public-key cryptosystem as a cryptosystem.
It is matter of course that...

...copyright management center 3 as the primary user information Iu1.
The database 1 prepares two **secret - keys** , that is, first **secret - key** Ks1 and second **secret - key** Ks2.
In the prepared first **secret - key** Ks1 and second **secret - key** Ks2,

the second **secret - key** Ks2 is also previously transferred to the copyright management center 3.

As the result of...

...to primary utilization, the primary user information Iu1, original copyright information Ic0 and the second **secret - key** Ks2 are stored in the copyright management center 3. In this case, the original copyright...

...request of the primary user. The read original data M0 is encrypted by the first **secret - key** Ks1: (Formula omitted)

The encrypted data Cm0ks1 is provided with the uncrypted original copyright information Ic0.

The first **secret - key** Ks1 is encrypted by the first public-key Kb1 and the second **secret - key** Ks2 is encrypted by the second public-key kb2: (Formula omitted) (Formula omitted)

While the **copyright** management program P is also **encrypted** by the **second secret - key** Ks2 (Formula omitted) the copyright management program P must not always be encrypted by the second **secret - key** Ks2 but it may be encrypted by any other proper crypt key.

The encrypted original data Cm0ks1, encrypted copyright management program Cpks2, and two encrypted **secret - keys** Cks1kb1 and Cks2kb2 are transferred to the primary riser terminal 4 via the communication network...

...from the database 1.

The primary user receiving the encrypted original data Cm0ks1, two encrypted **secret - keys** Cks1kb1 and Cks2kb2, and encrypted copyright management program Cpks2 from the database 1 decrypts the encrypted first **secret - key** Cks1kb1 by the database utilization software using the first private-key Kv1 corresponding to the first public-key Kb1: (Formula omitted) and decrypts the encrypted second **secret - key** Cks2kb2 using the second private-key Kv2 corresponding to the second public-key Kb2: (Formula omitted)

And the primary user **decrypts** the **encrypted copyright** management program Cpks2 using the **decrypted second secret - key** Ks2: (Formula omitted)

Finally, the primary user decrypts the **encrypted** data Cm0ks1 by the **decrypted copyright** management program P using the **decrypted first secret - key** Ks1: (Formula omitted) and uses the decrypted original data M0 directly or data M1 as...

...data M0 or the edited data M1, it is encrypted and decrypted by the second **secret - key** Ks2: (Formula omitted) (Formula omitted)

The decrypted second **secret - key** Ks2 is thereafter used as a crypt key for encrypting/decrypting data when storing, copying...

...transmitting the data.

The first private-key Kv1 and second private-key Kv2, the first **secret - key** Ks1 and second **secret - key** Ks2, the data M, the copyright management program P, the original copyright information Ic, and...

...to be distributed. Since the copyright information label provides a clue to obtain the second **secret - key** Ks2 which is the key for decryption, the second **secret key** Ks2 cannot be obtained in the case where the copyright information label is removed from...

...When the encrypted data Cmks2 is stored in the primary user terminal 4, the second **secret - key** Ks2 is stored in the terminal 4. However, when the encrypted data Cmks2 is not...

conference.

The video conference participant 122 receiving the first **secret - key** Ks1 generates the second **secret - key** Ks2 by the first **secret - key** Ks1 using the video conference data management program P:

The generated second **secret - key** Ks2 is stored in the terminal.

The video conference participant 121 encrypts the video conference data M0 with the first **secret - key** Ks1, in the video conference through the communication network 2: and transfers the encrypted video...

...video conference participant 122 who receives the video conference data Cm0ks1 encrypted by the first **secret - key** Ks1 decrypts the video conference data Cm0ks1 by the first **secret** - 1key Ks1: and uses decrypted video conference data M0.

Further, the second **secret - key** Ks2 is generated based on the first **secret - key** Ks1 with the video conference data management program P:

In the case where the decrypted...

...video conference via the communication network 2, the data M is encrypted by the second **secret - key** Ks2 using the video conference data management program P:

The encrypted data Cmks2 is copied...receives the request for the second use of the data M finds out the first **secret - key** Ks1 according to the name or the number of the video conference data name or number to generate the second **secret - key** Ks2 based on the first **secret - key** Ks1: and supplies the generated second **secret - key** Ks2 to the non-participant of the video conference 123.

The non-participant of video conference 123 who receives the second **secret - key** Ks2 decrypts the encrypted data Cmks2 by the second **secret - key** Ks2 by using the television conference data management program P: and then, uses decrypted video...

...of the video conference 124, the video conference data M is encrypted by the second **secret - key** Ks2 using the video conference data management program P:

Incidentally, the third **secret - key** Ks3 may be generated on the basis of the second **secret - key** Ks2 with the video conference data management program P: and the data M can be encrypted with the video conference data management program P by this generated third **secret - key** Ks3:

...CLAIMS in said read-only semiconductor memory;

a second private-key, a permit key, a second **secret - key** , a copyright management program, and copyright information are stored in said electrically erasable programmable memory...

...in said read-only semiconductor memory;

a second private-key, a permit key, a second **secret - key** , and copyright information are stored in said electrically erasable programmable memory; and

a first public...

14/3,K/38 (Item 36 from file: 348)

DIALOG(R)File 348:EUROPEAN PATENTS

00753646

Data copyright management system
Urheberrechtsdatenverwaltungssystem
Systeme de gestion de donnees de droits d'auteurs

PATENT ASSIGNEE:
MITSUBISHI CORPORATION, (653510), 6-3, Marunouchi 2-chome, Chiyoda-ku Tokyo 100, (JP), (applicant designated states: DE;FR;GB)
INVENTOR:
Saito, Makoto, 2-12-6-104, Kaitori, Tama-shi, Tokyo, (JP)
Momiki, Shunichi, 4-20-66, Kumegawa-cho, Higashimura-yama-shi, Tokyo, (JP)
LEGAL REPRESENTATIVE:
Heselberger, Johannes (156741), Patent- und Rechtsanwalte Bardehle . Pagenberg . Dost . Altenburg . Geissler Galileiplatz 1, 81679 Munchen, (DE)

PATENT (CC, No, Kind, Date): EP 709760 A2 960501 (Basic)
EP 709760 A3 990203
APPLICATION (CC, No, Date): EP 95116820 951025;
PRIORITY (CC, No, Date): JP 94264201 941027
DESIGNATED STATES: DE; FR; GB
INTERNATIONAL PATENT CLASS: **G06F-001/00** ; **G06F-012/14**
ABSTRACT WORD COUNT: 521

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPAB96	421
SPEC A	(English)	EPAB96	6978
Total word count - document A			7399
Total word count - document B			0
Total word count - documents A + B			7399

INTERNATIONAL PATENT CLASS: **G06F-001/00** ...

... **G06F-012/14**

...ABSTRACT is produced by editing a plurality of encrypted data obtained from the database, and is **encrypted** for **distribution** to another person, **crypt keys** for a **plurality** of data as raw material and an edition program which is an editing process with...

...comprises a database and a key control center, and uses a primary copyright label, a **first** use permit **key** including a **first** crypt **key** , a **second** use permit **key** , a third **crypt** key, and a **copyright** management program. The primary user uses primary **copyrighted** data **encrypted** by using the **first** crypt **key** and supplied, by decrypting it with the first use permit key obtained from the key...

...use permit key. At the completion of the editing, the primary user receives the third **crypt key** for **secondary copyright** as secondary exploitation right, **encrypts** the edited data with the third crypt key, and distributes it to a secondary user...

...new data is produced by editing a plurality of data obtained from the database, and **encrypted** for **distribution** to another person, **crypt keys** for a **plurality** of data as raw material and an edition program which is as an editing process...

...SPECIFICATION the key control center. On receiving the copyright management program Pc, the key control center **transfers** the **first crypt key** K1 and a **second** crypt **key** K2 corresponding to the

specific usage together with the copyright management program Pc to the ...copyright management program Pc which have been encrypted.
Typical means used for encrypting data include **secret - key** cryptosystem and public-key cryptosystem.

The **secret - key** cryptosystem uses the same secret crypt key Ks for both encryption and decryption:

CmKs = E...

...to the second public-key Kb2 which are prepared by the user, and a first **secret - key** Ks1 and a second **secret - key** Ks2 prepared by the database. The database uses the first **secret - key** Ks1 to encrypt data M

Cmks1 = E (Ks1, M)

and further encrypts the firstsecret-keys Ks1 by the first public-key Kb1

Cks1kb1 = E (Kb1, Ks1)

and encrypts the second **secret - key** Ks2 by the second public-key Kb2

Cks2kb2 = E (Kb2, Ks2);

the database then transmits these encrypted data Cmks1 and the first and the second **secret - keys** CKs1 and Cks2kb2 to the user;

the user decrypts the first **secret - key** Cks1kb1 using the first private-key

Kv1

Ks1 = D (Kv1, Cks1kb1),

and decrypts the encrypted data Cmks1 to use by decrypted first **secret - key** Ks1

M = D (Ks1, Cmks1),

and the encrypted second **secret - key** Cks2kb2 by the second private-key Kv2

Ks2 = D (Kv2, Cks2kb2);

and decrypted second **secret - key** Ks2 is used for data storage/copy/transfaer after data decryption.

SUMMARY OF THE INVENTION...user who requires encrypted secondary data requests the key control center for distributing the third **crypt** key. The key control center **distributes** the third **crypt key** to the **secondary** user.

The secondary user who receives the second crypt key decrypts encrypted secondary data using...

...to the second public-key Kb2 which are prepared by the user, and a first **secret - key** Ks1 and a second **secret - key** Ks2 prepared by the database. The database uses the first **secret - key** Ks1 to encrypt data

...use said primary copyrighted data requests distribution of said first use permit key to said **key** control center;

said **primary** user **decrypts** said primary **copyrighted** data for primary use by using said distributed first use permit key;

said primary user...

...from said key control center, and edits said primary copyrighted data by using said distributed **second** use permit **key** , said **copyrighted** data during editing being **encrypted** and stored by using said second use permit key;

said primary user who completes editing...

14/3,K/39 (Item 37 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00747145
Data copyright management system
Datenurheberrechtsverwaltungssystem
Systeme de gestion des droits d'auteur de donnees
PATENT ASSIGNEE:
MITSUBISHI CORPORATION, (653510), 6-3, Marunouchi 2-chome, Chiyoda-ku, Tokyo 100-0005, (JP), (Proprietor designated states: all)
INVENTOR:
Saito, Makoto, 2-12-6-104, Kaitori, Tama-shi, Tokyo, (JP)
Momiki, Shunichi, 4-20-66, Kumegawa-cho, Higashimurayama-shi, Tokyo, (JP)
LEGAL REPRESENTATIVE:
Pfenning, Meinig & Partner GbR (100967), Mozartstrasse 17, 80336 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 704785 A2 960403 (Basic)
EP 704785 A3 990825
EP 704785 B1 031119
APPLICATION (CC, No, Date): EP 95115068 950925;
PRIORITY (CC, No, Date): JP 94237673 940930; JP 94264199 941027; JP 94269959 941102
DESIGNATED STATES: DE; FR; GB
INTERNATIONAL PATENT CLASS: **G06F-001/00** ; G07F-007/10; **G06F-012/14**
ABSTRACT WORD COUNT: 292
NOTE:
Figure number on first page: 1

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPAB96	3024
CLAIMS B	(English)	200347	712
CLAIMS B	(German)	200347	616
CLAIMS B	(French)	200347	935
SPEC A	(English)	EPAB96	23788
SPEC B	(English)	200347	23328
Total word count - document A			26817
Total word count - document B			25591
Total word count - documents A + B			52408

INTERNATIONAL PATENT CLASS: **G06F-001/00** ...

...SPECIFICATION transfers the third secret-key Ks3 serving as a decryption key and the fourth secret- **key** Ks4 serving as an encryption/decryption key to the tertiary user terminal 6 via the communication network 8.

In the tertiary user terminal 6 receiving the third **secret - key** Ks3 and the fourth **secret - key** Ks4, the encrypted data Cmks3 is decrypted using the third **secret - key** Ks3 by the copyright management program P (Formula omitted) and is tertiarily utilized such as...

...this embodiment, the data M supplied to a primary user is encrypted by the first **secret - key** Ks1 and the data M supplied to a secondary user is encrypted by the second **secret - key** Ks2, and the data M supplied to a tertiary user is encrypted by the third **secret - key** Ks3.

Therefore, if the tertiary user, instead of the primary user, falsely requests for primary utilization to the key control center 9, the first **secret - key** Ks1 for decryption and the **second secret - key** Ks2 for **encryption / decryption** are **transferred** to the tertiary user. However, it is impossible to decrypt the encrypted data Cmks3 by the **first secret - key** Ks1 **transferred** as a **decryption** key.

Moreover, if the tertiary user, instead of the secondary user, falsely requests for secondary utilization to the key control center 9, the second **secret - key** Ks2 and the third **secret - key** Ks3 are transferred to the tertiary user as a decryption key and an encryption/decryption key respectively. However, it is impossible to decrypt the encrypted data CmKs3 by the **second secret - key** Ks2 **transferred** as a **decryption** key.

Therefore, it is impossible to falsely request for data utilization. As a result, not...

...of the first embodiment, a copyright management program and, if circumstances require, first and second **secret - keys** are encrypted and supplied.

Also in the case of this embodiment, similarly to the case...

...recording medium 3, or communication network 8. The data M0 is encrypted by the first **secret - key** Ks1: (Formula omitted)

A primary user who desires primary utilization of the supplied encrypted data...

...receiving the request of the primary utilization of the encrypted original data Cm0ks1 generates a **secret - key** Ksu1 unique to the primary user using the primary user information Iu1 and transfers it to the copyright management center 10.

The copyright management center 10 receiving the **primary** user unique **secret - key** Ksu1 **encrypts** the **copyright** management program P by using the primary user unique **secret - key** Ksu1 (Formula omitted) and transfers an encrypted copyright management program Cpksu1 to the key control...

...generated is inherent in the primary user.

The key control center 9 transfers the first **secret - key** Ks1 for decryption and the second **secret - key** Ks2 for decryption/encryption to the primary user terminal 4 via the communication network 8...

...received from the copyright management center 10.

In the primary user terminal 4 receiving the **encrypted copyright** management program Cpksu1, **first secret - key** Ks1, and **second secret - key** Ks2, database system software S previously distributed generates a primary user unique **secret - key** Ksu1 in accordance with

In the case where...

...video conference via the communication network 8, the data M is encrypted by the second **secret - key** Ks2 using the video conference data management program P: (Formula omitted)

The encrypted data Cmks2...

...receives the request for the second use of the data M finds out the first **secret - key** Ks1 according to the name or the number of the video conference data name or number to generate the second **secret - key** Ks2 based on the first **secret - key** Ks1: (Formula omitted) and supplies the generated second **secret - key** Ks2 to the non-participant 46 of the video conference.

The non-participant 46 of video conference who receives the second **secret - key** Ks2 decrypts the encrypted data Cmks2 by the second **secret - key** Ks2 by using the television conference data management program P: (Formula omitted) and then, uses...

...47 of the video conference, the video conference data M is encrypted by the second **secret - key** Ks2 using the video conference data management program P: (Formula omitted)

Incidentally, the third **secret - key** Ks3 may be generated on the basis of the second **secret - key** Ks2 with the television conference data management program P: (Formula omitted) and the data M can be encrypted with the video conference data management program P by this generated third **secret - key** Ks3: (Formula omitted)

In embodiment 19 described above, the constitution of the data copyright management...

...Figure 4 for realizing the video conference data management system is applied and alter the **secret - key** which has been used.

However, as a constitution of a system for realizing the video...

...5 can be applied. Further, as cryptosystem used in such a case, the non-altered **secret - key** , the public-key and the private-key, a combination of the **secret - key** , the public-key and the private-key, and the complex keying which is explained from...

...only normal communication software such as a data communication protocol but also a program for **decrypting** a **copyright** management program by a **first crypt key** , it is necessary to be protected.

In case of the present invention, a **first** crypt **key** K1, a **second crypt key** K2, and a **copyright** management program P are transferred to each user in order to use data M. Therefore...

...private-key in the public-key cryptosystem and the program containing algorithm for generating the **secret - key** are kept when needed.

For keeping them, it is the simplest means to use a...

...software and user data as a database.

The read-only memory 55 also stores a **first** crypt **key** , a **second crypt key** , and a **copyright** management program supplied from a key control center 9 or a copyright management center. Because...

14/3,K/40 (Item 38 from file: 348)

00733499

COMPUTER NETWORK CRYPTOGRAPHIC KEY DISTRIBUTION SYSTEM

KRYPTOGRAPHISCHES SCHLUSSELVERTEILUNGSSYSTEM IN EINEM RECHNERNETZ
SYSTEME DE DISTRIBUTION DE CLE CRYPTOGRAPHIQUE POUR RESEAU INFORMATIQUE
PATENT ASSIGNEE:
ENTRUST TECHNOLOGIES LTD., (2538870), 750 Heron Road, Tower E, Ottawa, Ontario K2G 5J9, (CA), (applicant designated states: BE;DE;FR;GB;IT;NL)
INVENTOR:
FORD, Warwick, Stanley, 25 Assiniboine Drive, Nepean, Ontario K2E 5R8, (CA)
WIENER, Michael, James, 20 Hennepin Street, Nepean, Ontario K2J 3Z4, (CA)
LEGAL REPRESENTATIVE:
Newstead, Michael John et al (34352), Page Hargrave Temple Gate House Temple Gate, Bristol BS1 6PL, (GB)
PATENT (CC, No, Kind, Date): EP 755598 A1 970129 (Basic)
EP 755598 B1 980916
WO 9528784 951026
APPLICATION (CC, No, Date): EP 95908852 950222; WO 95CA84 950222
PRIORITY (CC, No, Date): US 227871 940415
DESIGNATED STATES: BE; DE; FR; GB; IT; NL
INTERNATIONAL PATENT CLASS: H04L-009/08; **G06F-012/14**
NOTE:
No A-document published by EPO
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	9838	1026
CLAIMS B	(German)	9838	883
CLAIMS B	(French)	9838	1277
SPEC B	(English)	9838	5283
Total word count - document A			0
Total word count - document B			8469
Total word count - documents A + B			8469

...INTERNATIONAL PATENT CLASS: **G06F-012/14**

...SPECIFICATION each user is assigned a pair of matching secret and public keys. Each user's **secret key** is broken into shares. Each user then provides a plurality of trustees pieces of information which enables each trustee to verify its share of the **secret key** . Thus all the trustees must agree to reveal to a third party the **secret key** of a user.
EP0343805, published November 29, 1989 describes techniques of reproducing secure keys by...
...prekey. Key generation data are divided into more than one part and each part is **encrypted** in a **distributed** fashion, **first** by a **first key** prekey to obtain a symmetric key by which information is scrambled before transmission.
The present...

14/3,K/41 (Item 39 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00262447
Manipulating rights-to-execute in connection with a software copy protection mechanism.
Behandlung von Ausfuhrungsrechten mit Bezug auf einen Softwarekopierschutzmechanismus.
Manipulation des droits d'execution a propos d'un mecanisme de protection de logiciel contre copie.
PATENT ASSIGNEE:

International Business Machines Corporation, (200120), Old Orchard Road, Armonk, N.Y. 10504, (US), (applicant designated states: DE;FR;GB;IT)
INVENTOR:
Comerford, Liam David, Box 191 Rd. No. 1 10 Valley Road, Carmel, N.Y. 10512, (US)
White, Steve Richard, 7 Park Avenue Apt. 33, New York, N.Y. 10016, (US)
LEGAL REPRESENTATIVE:
Burt, Roger James, Dr. et al (52152), IBM United Kingdom Limited Intellectual Property Department Hursley Park, Winchester Hampshire SO21 2JN, (GB)
PATENT (CC, No, Kind, Date): EP 268139 A2 880525 (Basic)
EP 268139 A3 910410
APPLICATION (CC, No, Date): EP 87116179 871103;
PRIORITY (CC, No, Date): US 927299 861105
DESIGNATED STATES: DE; FR; GB; IT
INTERNATIONAL PATENT CLASS: **G06F-012/14** ; **G06F-001/00**
ABSTRACT WORD COUNT: 137

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPABF1	2301
SPEC A	(English)	EPABF1	17139
Total word count - document A			19440
Total word count - document B			0
Total word count - documents A + B			19440

INTERNATIONAL PATENT CLASS: **G06F-012/14** ...

... **G06F-001/00**

...SPECIFICATION this sensitive information from unauthorized persons. The same data is encrypted under a hardware manufacturer **secret key** called a Common Supervisor Key (CSK) to generate E(sub(CSK))(token data). It is...B. As Fig. 1 shows the application file B is encrypted under the software decryption **key** AK. A **second** file on the **distribution** disk 16 is the software **decryption** key, encrypted under the key CSK. Finally, the last file on the distribution disk is... computing system to provide for the encryption of token data and software under his own **secret key** (AK) in accordance with the software protection mechanism described in copending application (YO985-091), another...

14/3,K/42 (Item 40 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2005 European Patent Office. All rts. reserv.

00171794
Method of software protection.
Softwaresicherungsverfahren.
Procede de protection de logiciel.
PATENT ASSIGNEE:
International Business Machines Corporation, (200120), Old Orchard Road, Armonk, N.Y. 10504, (US), (applicant designated states: DE;FR;GB;IT)
INVENTOR:
Matyas, Stephen Michael, R.D. 5 Box 19F, Kingston New York 12401, (US)
Oseas, Jonathan, Box 147, Hurley New York 12401, (US)
LEGAL REPRESENTATIVE:
Bailey, Geoffrey Alan (27921), IBM United Kingdom Limited Intellectual

Property Department Hursley Park, Winchester Hampshire SO21 2JN, (GB)
PATENT (CC, No, Kind, Date): EP 191162 A2 860820 (Basic)
EP 191162 A3 890308
EP 191162 B1 930203
APPLICATION (CC, No, Date): EP 85115147 851129;
PRIORITY (CC, No, Date): US 682854 841218
DESIGNATED STATES: DE; FR; GB; IT
INTERNATIONAL PATENT CLASS: **G06F-012/14** ; G07F-007/00; G07F-007/10
ABSTRACT WORD COUNT: 233

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	EPABF1	1501
SPEC B	(English)	EPABF1	9028
Total word count - document A			0
Total word count - document B			10529
Total word count - documents A + B			10529

INTERNATIONAL PATENT CLASS: **G06F-012/14** ...

...SPECIFICATION and a secret computer key. However, the public computer key is first decrypted under the **secret key** of the computer manufacturer and stored in the computer in that form. When the program...

...pair; i.e, a secret computer key and a public computer key decrypted under the **secret key** of the designated public registry. The advantage to this approach is that the file key...press-on label visible to the user. This identification or number is associated with the **secret key** of the crypto facility of the computer. The program number and the diskette serial number...simply encrypts the provided program number and diskette serial number, concatenated together, with a special **secret key** , SK, used only to generate multi-digit authorisation numbers. The n-bit portion of the...encryption key, KP, from table 27. Alternatively, the key KP can be generated from a **secret key** belonging to the key distribution centre in a similar manner as the eKT(TR) keys are generated using **secret key** KT as shown in Figure 3. This encryption key is then used to encrypt the...implementation containing the Data Encryption Standard (DES) algorithm and storage for a small number of **secret keys** . It can be accessed logically only through inviolate interfaces secure against intrusion, circumvention and deception...
...personal computer and smart card with no loss of security to protected software or the **secret keys** or parameters that support the system. To interface to the system, it is only necessary...

...this embodiment, the main advantage of the PK algorithm is achieved, namely that a universal **secret key** need not be stored on the smart card. The card manufacturer personalises the card with...the computer with a unique key pair, the computer public key, PKt, and the computer **secret key** , SKt. The computer manufacturer has the public key of the computer recorded in a public...

...this means that PKt is stored in the form dSu(PKt), where SKu is the **secret key** of the registry and PKt is the public key of the computer. This value dSu...

...several redundancy bits (0 bits in this case) concatenated with it is decrypted under the **secret key** SKu. SKu is the **secret key** belonging to the computer manufacturer. The redundancy bits are added to the message so that...

...101 of the computer 10 where it is decrypted in decryption block 105 using the **secret key** , SKt, of the computer and then exclusive ORed with the random number T. The file...

...properly recorded in the registry, i.e. for which PKt has been deciphered under the **secret key** of the registry.
The advantages of the mixed public key and DES embodiment are several ...

...with no loss in security to the protected software of a given vendor or the **secret keys** or parameters that support the system. To interface to the system, it is only necessary...constant of sufficient bits which may have a value of zero all decrypted under the **secret key** , SKu, of the distribution centre.
Also with the smart card, a third operation shown in...constant of sufficient bits which may have a value of zero all decrypted under the **secret key** , SKu, of the distribution centre. Used in conjunction with the second operation, the seventh operation...

...CLAIMS identifier and then encrypting the program number and storage medium number concatenated together with said **first key** to produce a **second key** at the **key distribution** centre, and **encrypting** the secret file key of the program with said second key to produce said password...further comprising the steps providing the computer with a public key, PKt, decrypted under the **secret key** of a public registry, and also providing said cryptographic facility with a corresponding **secret key** , SKt, providing said smart card with a public key, PKu, encrypting in the smart card the computer public key decrypted under the **secret key** of the public registry with the card's public key PKu to produce said key...

14/3,K/43 (Item 1 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01251974 **Image available**
METHODS AND APPARATUSES FOR DISTRIBUTING SYSTEM SECRET PARAMETER GROUP AND ENCRYPTED INTERMEDIATE KEY GROUP FOR GENERATING CONTENT ENCRYPTION AND DECRYPTION DEYS
PROCEDES ET APPAREILS PERMETTANT DE DISTRIBUER UN GROUPE DE PARAMETRES SYSTEME SECRETS ET UN GROUPE DE CLES INTERMEDIAIRES CRYPTEES AFIN DE GENERER DES CLES DE CRYPTAGE ET DECRYPTAGE DE CONTENU
Patent Applicant/Assignee:
MATSUSHITA ELECTRIC INDUSTRIAL CO LTD, 1006, Oaza Kadoma, Kadoma-shi, Osaka, 5718501, JP, JP (Residence), JP (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
NONAKA Masao, -- (Residence), -- (Nationality), (Designated only for: US)
FUTA Yuichi, -- (Residence), -- (Nationality), (Designated only for: US)
OHMORI Motoji, -- (Residence), -- (Nationality), (Designated only for: US)
YAMADA Shigeru, -- (Residence), -- (Nationality), (Designated only for: US)
INOUE Tetsuya, -- (Residence), -- (Nationality), (Designated only for: US)
KUMAZAKI Yoji, -- (Residence), -- (Nationality), (Designated only for: US)
Legal Representative:

NII Hiromori (agent), c/o NII Patent Firm, 3rd Floor, Shin-Osaka Suehiro Center Bldg., 11-26, Nishinakajima 3-chome, Yodogawa-ku, Osaka-shi, Osaka 532-0011, JP,

Patent and Priority Information (Country, Number, Date):
Patent: WO 200559727 A1 20050630 (WO 0559727)
Application: WO 2004JP19141 20041215 (PCT/WO JP04019141)
Priority Application: JP 2003419766 20031217

Designated States:
(All protection types applied unless otherwise stated - for applications 2004+)
AE AG AL AM AT AU AZ BA BB BG BR BW BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE EG ES FI GB GD GE GH GM HR HU ID IL IN IS KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NA NI NO NZ OM PG PH PL PT RO RU SC SD SE SG SK SL SY TJ TM TN TR TT TZ UA UG US UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LT LU MC NL PL PT RO SE SI SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) BW GH GM KE LS MW MZ NA SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English
Filing Language: English
Fulltext Word Count: 47576

Main International Patent Class: **G06F-001/00**
Fulltext Availability:
Detailed Description
Claims

Detailed Description
... individual key given to each of the content output apparatuses so as to generate a **plurality** of **encrypted** intermediate **key** groups; and **distributing** ,, to the content output -13 apparatuses, an encrypted intermediate key group set that is made...when it receives the encrypted intermediate key group set ENCMKGS from the intermediate key group **encryption** unit 115, **distributes** the received **encrypted** intermediate **key** group set ENCMKGS to the **plurality** of output apparatuses 13a to 13n via the communication path 10,
(7) Input Unit 117...

...group encryption unit 115 outputs the generated encrypted intermediate key group set ENCMKGS to the **encrypted** intermediate key group set **distribution** unit 116 (S1112).

The **encrypted** intermediate key group set **distribution** unit 116 receives the **encrypted** intermediate key group set ENCMKGS, **distributes** the received **encrypted** intermediate **key** group set ENCMKGS to the **plurality** of output apparatuses 13a to 13n, and terminates the operation (S1113).

<<Operation at Revoking Output...Group Storage Unit 127
The system secret parameter group storage unit 127 holds the system **secret** **key** group SPG as shown in FIG. 12. The system secret parameter group receiving unit 126...nent has an effect that the key issuing center 21 can reduce the frequency of **distributing** the **encrypted** intermediate **key** group set EMCMKGS to the **plurality** of output apparatuses 22a to 22n by embedding sets of intermediate key groups in the...unit 616 (S6112).

The encrypted intermediate key group set d.istribution unit 616 receives the **encrypted** intermediate key group set ENCMKGS, **distributes** the received **encrypted** intermediate **key** group set ENCMKGS to the **plurality** of output apparatuses 63 a to 63n and terminates the process (S6113).

They are the...CK2 based on the content key CK, further encrypts the content CNT based on the **second** content **key** CK2 and **distributes** the **encrypted** content ENCCNT and the encrypted second content key CK2 to the output apparatuses 63a to...

...content key CK3. encrypt the content CNT based on the third content key CK3, and **distribute** the **encrypted** content ENCCNT, **second** content **key** CK2 and third content key CK3 to the output apparatuses 63a to 63n.

It may...

Claim
... individual key given to each of the content output apparatuses so as to generate a **plurality** of **encrypted** intermediate **key** groups; and
distributing , to the content output apparatuses, an encrypted intermediate key group set that is made up...

...individual key given to each of the content output apparatuses so as to generate a **plurality** of **encrypted** intermediate **key** groups; and
distributing , to the content output apparatuses,, an encrypted intermediate key group set that is made up...

14/3,K/44 (Item 2 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01169937 **Image available**
METHOD AND SYSTEM FOR MANAGING DIGITAL RIGHTS
PROCEDE ET SYSTEME DE GESTION DES DROITS NUMERIQUES
Patent Applicant/Assignee:
KONINKLIJKE PHILIPS ELECTRONICS N V, Groenewoudseweg 1, NL-5621 BA Eindhoven, NL, NL (Residence), NL (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
FONTIJN Wilhelmus F J, c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven, NL, NL (Residence), NL (Nationality), (Designated only for: US)
Legal Representative:
GROENENDAAL Antonius W M (agent), Prof. Holstlaan 6, NL-5656 AA Eindhoven , NL,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200492931 A2-A3 20041028 (WO 0492931)
Application: WO 2004IB50429 20040414 (PCT/WO IB04050429)
Priority Application: EP 2003101065 20030417
Designated States:
(All protection types applied unless otherwise stated - for applications 2004+)
AE AG AL AM AT AU AZ BA BB BG BR BW BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE EG ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NA NI NO NZ OM PG PH PL PT RO

RU SC SD SE SG SK SL SY TJ TM TN TR TT TZ UA UG US UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PL PT RO SE SI SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) BW GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 5056

Main International Patent Class: **G06F-001/00**
Fulltext Availability:
Detailed Description

Detailed Description
... content item or a part of the content item. A digital right may comprise a **plurality** of content **decryption keys** . Alternatively, a **digital right** may comprise a small software application which is able to generate content decryption keys. Advantageously...
...integrated circuit of the method as well as re-encrypt the digital right using a **secret key** that is only known to authorized integrated circuits. This provides a high level of security...

14/3,K/45 (Item 3 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01161905 **Image available**
REMOTE ACCESS AUTHORIZATION OF LOCAL CONTENT
AUTORISATION D'ACCES A DISTANCE A UN CONTENU LOCAL
Patent Applicant/Assignee:
C14 TECHNOLOGIES INC, 1327 Chesapeake Terrace, Sunnyvale, CA 94089, US, US (Residence), US (Nationality), (For all designated states except: US)
Inventor(s):
CHAN Man, 3275 Moulin Lane, San Jose, CA 95135, US,
Legal Representative:
YOUNG Barry N (agent), Gray Cary Ware & Freidenrich, 2000 University Avenue, East Palo Alto, CA 94303, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200484008 A2-A3 20040930 (WO 0484008)
Application: WO 2004US6698 20040303 (PCT/WO US04006698)
Priority Application: US 2003392591 20030318
Designated States:
(All protection types applied unless otherwise stated - for applications 2004+)
AE AG AL AM AT AU AZ BA BB BG BR BW BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE EG ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NA NI NO NZ OM PG PH PL PT RO RU SC SD SE SG SK SL SY TJ TM TN TR TT TZ UA UG US UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PL PT RO SE SI SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) BW GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 10802

International Patent Class: **G06F-017/60**

Fulltext Availability:
  Detailed Description
  Claims

Detailed Description
... process creates the encrypted content C'i by using the encryption algorithm Ei and the **secret key** Ki to process the plaintext content Ci in a well known manner. There is associated...

...algorithm a decryption algorithm, Di, such that when the encrypted content C'i and the **secret key** Ki are processed using the decryption algorithm, the plain text content Ci is returned, i...

Claim
... remote server said information provided to the user using a first encrypting process and a **first encryption key** ; and **downloading** to a browser at the user a page containing said encrypted information.

5 The method...

14/3,K/46 (Item 4 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2005 WIPO/Univentio. All rts. reserv.

01155871
SYSTEM FOR ON-LINE AND OFF-LINE DECRYPTION
SYSTEME DE DECRYPTAGE EN LIGNE ET HORS LIGNE
Patent Applicant/Assignee:
  SECURE DATA IN MOTION INC, 1875 South Grant Street, Suite 500, San Mateo, CA 94402, US, US (Residence), US (Nationality)
Inventor(s):
  MOREH Jahanshah, 2122 Century Park Lane, Apt. 417, Los Angeles, CA 90067, US,
  BRUNS Logan O'Sullivan, 127 Quarry Drive, Napa, CA 94559, US,
Legal Representative:
  ROBERTS Raymond E (agent), Intellectual Property Law Offices, 1901 South Bascom Avenue, Suite 660, Campbell, CA 95008, US,
Patent and Priority Information (Country, Number, Date):
  Patent: WO 200477290 A1 20040910 (WO 0477290)
  Application: WO 2003US19953 20030625 (PCT/WO US03019953)
  Priority Application: US 2003449068 20030220; US 2003250004 20030527
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
  AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ
  EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR
  LS LT LU LV MA MD MG MK MN MW MX MZ NI NO NZ OM PG PH PL PT RO RU SC SD
  SE SG SK SL TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW
  (EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT RO SE
  SI SK TR
  (OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
  (AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
  (EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 7155

Main International Patent Class: **G06F-009/00**
Fulltext Availability:
  Detailed Description

Detailed Description
... key server delivers the message key to the recipient, which uses the message key to **decrypt** the email.

Distributing symmetric **keys** via a **key** server has **many** positive attributes. For example, a sender (or any authorized party) can determine when a recipient...

...key that encrypts the message key and an envelop decryption key is the private or **secret** **key** that decrypts the message key.

Key exchange algorithm means the algorithm a sender and the...

14/3,K/47 (Item 5 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01012869 **Image available**
DEVICE AND METHOD WITH REDUCED INFORMATION LEAKAGE
DISPOSITIF ET PROCEDE POUR LIMITER LA FUITE D'INFORMATIONS
Patent Applicant/Assignee:
INTERNATIONAL BUSINESS MACHINES CORPORATION, New Orchard Road, Armonk, NJ 10504, US, US (Residence), US (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
BAENTSCH Michael, Wildenbuehlstrasse 13, CH-8135 Langnau am Albis, CH, CH (Residence), DE (Nationality), (Designated only for: US)
BUHLER Peter, Muehlestrasse 39, CH-8803 Rueschlikon, CH, CH (Residence), DE (Nationality), (Designated only for: US)
EIRICH Thomas, Robert-Walser-Strasse 50, CH-8820 Waedenswil, CH, CH (Residence), DE (Nationality), (Designated only for: US)
HOERING Frank, Culmannstrasse 39, CH-8006 Zurich, CH, CH (Residence), DE (Nationality), (Designated only for: US)
OESTREICHER Marcus, Kalkbreitestrasse 120, CH-8003 Zurich, CH, CH (Residence), DE (Nationality), (Designated only for: US)
WEIGOLD Thomas D, Buttenaustrasse 20, CH-8134 Adliswil, CH, CH (Residence), DE (Nationality), (Designated only for: US)
Legal Representative:
TOLETI Martin (agent), International Business Machines Corporation, Saeumerstrasse 4 / Postfach, CH-8803 Rueschlikon, CH,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200342799 A2-A3 20030522 (WO 0342799)
Application: WO 2002IB4620 20021105 (PCT/WO IB0204620)
Priority Application: EP 2001811093 20011114
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ
EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR
LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI
SK SL TJ TM TN TR TT TZ UA UG US UZ VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 9400

Main International Patent Class: **G06F-001/00**
Fulltext Availability:
Detailed Description

Detailed Description
... of processes such as data encryption and authentication. In a typical symmetric cryptographic process, a **secret key** is known ...In systems using asymmetric or public-key cryptography, one party typically performs operations using a **secret key** , e.g., the so-called private key, while the other performs complementary operations using only...as described for example by E. Biham and A. Shamir in "Differential Fault Analysis of **Secret Key** Cryptosystems," Advances in Cryptology--CRYPTO '97, ...uses the same key to transforrn ciphertext blocks into their corresponding plaintexts.

To obtain a **secret key** from ...maintain and manipulate secret parameters in open environments without revealing their values. Compromise of a **secret key** used to compute a digital signature could, for example, allow an attacker to forge the...being manipulated within it. Such signals can be measured and analyzed by attackers to recover **secret keys** . State transitions are also a major ...amount of power consumed when the system is in transition. Attackers can non-invasively extract **secret keys** using external measurement and analysis of a device's power consumption, electromagnetic radiation, or processor... fluctuations, DPA attacks use statistical analysis and error correction techniques to extract information correlated to **secret keys** . Hence, DPA is a much more powerful attack than SPA, and ...lookup at a time, it is only necessary to guess the six bits of the **secret key** that are relevant to the S-box being observed and corresponding to the power consumption possible sequences of values for a given 6-bit portion of the 56-bit **secret key** . For each guess of the values of these six bits, one divides the samples into...the six key bits was incorrect. This process of guessing at the value of the **secret key** , dividing the power signature samples into those which will yield a 1-output and those ...remaining key space of 21 = 256 possible keys to find the balance of the correct **secret key** . It becomes apparent how little information the attacker needs to employ such an attack. The...indexed key update technique are disclosed. In one embodiment, a cryptographic client device maintains a **secret key** value as part of its state. The client can update its secret value at any...power consumption, and the actual EEPROM contents are derived. If such EEPROM content is a **secret key** guarding an electronic transaction for example, the security of the whole electronic transaction system is...20 and that suffers from the information - 19 leakage of the EEPROM 20, namely the **second cryptographic key** 21, is **transferred** in **encrypted** form. Since the leakage of the ROM 40 and the RAM 30 is lower than...prone to the attack stated above. The encryption step is performed under use of another **secret key** , the cryptographic master key 45, that may either be unique to the chip, or unique...

14/3,K/48 (Item 6 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00916583 **Image available**
AUTHENTICATION IN A CRYPTO-SYSTEM
AUTHENTIFICATION DANS UN SYSTEME DE CHIFFREMENT
Patent Applicant/Assignee:
SINGLESIGNON NET, 11417 Sunset Hills Road, Suite 105, Reston, VA 20190,

US, US (Residence), US (Nationality)
Inventor(s):
SANDHU Ravi, 3507 Majestic Pine Lane, Fairfax, VA 22033, US,
DESA Colin, 1096 Liberty Meeting Court, Herndon, VA 20170, US,
GANESAN Karuna, 5240 Blue Yarrow Run, Norcross, GA 30092, US,
Legal Representative:
STADNICKI Alfred A (agent), 1146 Nineteenth Street, N.W., 5th floor, Washington, DC 20036, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200250677 A1 20020627 (WO 0250677)
Application: WO 2001US48097 20011218 (PCT/WO US0148097)
Priority Application: US 2000739118 20001219
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
JP
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
Publication Language: English
Filing Language: English
Fulltext Word Count: 16737

Main International Patent Class: **G06F-001/24**
Fulltext Availability:
Detailed Description

Detailed Description
... symmetric key cryptography, the two parties who want to communicate in private share a common **secret key** , say K. the sender encrypts messages with K, to generate a cipher, i.e. C...for any message M of his choice since the computation is based on a shared **secret key** . With digital signatures this is not possible since only the sender has knowledge of the...The network station receiving the first
authentication request is the network station which generates and **distributes** the shared symmetric **crypto - key** . Thus, both the **second**

D and third network stations can perform identical operations. In one beneficial aspect of the...preferably are associated with a sponsor. A sponsor
is an entity controlling generation, assignment, and **distribution** of the asymmetric **crypto - keys** . Furthermore, either the **first** or the second network station can be the network station having generated t-he asymmetric...user's portion of the private key. Cl can than be used as a shared **secret key** between the user and the sponsor stations. Thus, by demonstrating knowledge of C1, the user...

14/3,K/49 (Item 7 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2005 WIPO/Univentio. All rts. reserv.

00913727 **Image available**
ELECTRONIC VOTING SYSTEM
SYSTEME DE VOTE ELECTRONIQUE
Patent Applicant/Assignee:
THE UNIVERSITY OF NORTH CAROLINA AT GREENSBORO, P.O. Box 26170, Greensboro, NC 27402-6170, US, US (Residence), US (Nationality)
Inventor(s):
KARRO Jared, Dept. of Mathematical Sciences/338 Bryan Building, Greensboro, NC 27402, US,

WANG Jie, Dept. of Mathematical Sciences/338 Bryan Building, Greensboro, NC 27402, US,
Patent Applicant/Inventor:
KARRO Jared, Dept. of Mathematical Sciences/338 Bryan Building, Greensboro, NC 27402, US, US (Residence), US (Nationality)
WANG Jie, Dept. of Mathematical Sciences/338 Bryan Building, Greensboro, NC 27402, US, US (Residence), US (Nationality)
Legal Representative:
ANTOLIN Stanislav (agent), Maccord Mason PLLC, P.O. Box 2974, Greensboro, NC 27402, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200246883 A2-A3 20020613 (WO 0246883)
Application: WO 2001US48357 20011205 (PCT/WO US0148357)
Priority Application: US 2000731035 20001206
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PH PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 25162

Main International Patent Class: **G06F-017/60**
Fulltext Availability:
Detailed Description
Claims
Detailed Description
... data in the distributor database. A preferred distributor database encryptor includes an on the fly **encryptor** . The 8
distributor database **encryptor** preferably uses public **keys** generated by a **plurality** of facilities of the election system to encrypt the distributor database.

Decryption of data within...the only way to completely decode a piece of data would be to acquire the **secret** **keys** of all severs, which, by our assumption, is impossible. Because the database is encrypted piece...

...a randomly selected third facility C. Facility C then decrypts the data with its own **secret** **key** , verifies that the size and the structure of the data it received have not been...We first prove the following lemma.

Lemma 1. If no facility knows all other facilities' **secret** **keys** , then any collaboration among facilities can be detected by a non-collaborating facility.

Proof. We...

Claim
... the only way to completely decode a piece of data would be to acquire the **secret** **keys** of all severs, which, by our assumption, is impossible. Because the database is encrypted piece...

...a randomly selected third facility C. Facility C then decrypts the data

with its own **secret key** , verifies that the size and 5- the structure of the data it received have not...on the fly encryptor.
5 1
. The election system according to Claim 39 wherein said **distributor** database **encryptor** uses public **keys** generated by a **plurality** of facilities of said election system to
encrypt said matcher database.

42 The election system...the fly encryptor. 1 5 146. The election system according to Claim 144 wherein said **distributor** database **encryptor** uses public **keys** generated by a **plurality** of facilities of said election system to encrypt said matcher database. 147. The election system...

14/3,K/50 (Item 8 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00876811 **Image available**
SYSTEM, METHOD AND COMPUTER PROGRAM PRODUCT FOR DEVICE, OPERATING SYSTEM, AND NETWORK TRANSPORT NEUTRAL SECURE INTERACTIVE MULTI-MEDIA MESSAGING
SYSTEME, PROCEDE ET PRODUIT PROGRAMME D'ORDINATEUR POUR APPAREIL, SYSTEME D'EXPLOITATION ET MESSAGERIE MULTIMEDIA INTERACTIVE RESEAU, NEUTRE ET SECURISEE
Patent Applicant/Assignee:
STORYMAIL INC, 15729 Los Gatos Boulevard, Los Gatos, CA 95032, US, US (Residence), US (Nationality)
Inventor(s):
ILLOWSKY Daniel H, 21363 Dexter, Cuptertino, CA 95014, US,
WENOCUR Michael L, 4057 Amaranta Avenue, Palo Alto, CA 94306, US,
BALDWIN Robert W, 990 Amarillo Avenue, Palo Alto, CA 94303, US,
SAXBY David B, 14946 Granite Court, Saratoga, CA 95070, US,
Legal Representative:
ANANIAN R Michael (et al) (agent), Flehr Hohbach Test Albritton & Herbert LLP, 4 Embarcadero Center, Suite 3400, San Francisco, CA 94111-4187, US
,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200210962 A1 20020207 (WO 0210962)
Application: WO 2001US23713 20010727 (PCT/WO US0123713)
Priority Application: US 2000627357 20000728; US 2000627358 20000728; US 2000627645 20000728; US 2000628205 20000728; US 2000706606 20001104; US 2000706609 20001104; US 2000706610 20001104; US 2000706611 20001104; US 2000706612 20001104; US 2000706613 20001104; US 2000706614 20001104; US 2000706615 20001104; US 2000706616 20001104; US 2000706617 20001104; US 2000706621 20001104; US 2000706661 20001104; US 2000706664 20001104; US 2001271455 20010225; US 2001912715 20010725; US 2001912936 20010725; US 2001912905 20010725; US 2001912773 20010725; US 2001912885 20010725; US 2001912860 20010725; US 2001912941 20010725; US 2001912901 20010725; US 2001912772 20010725
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW

(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 169299

Main International Patent Class: **G06F-017/00**
Fulltext Availability:
Detailed Description
Claims

Detailed Description
... for sending in an email message.

This algorithm performs three block encryption algorithms using a **secret key** , called Kmt, chosen by the server during installation. If this key is compromised, then the...

...XTEA, which has a 128-bit key.

If the server needs to change the Kmt **secret key** , it will not be able to recognize MTs created by the old key. However, if...can be expressed as a function as show immediately below. In one embodiment, the Data-**Encryption - Key** is the **first** 128-bits of the 160-bit OAEP-Seed. SealSignedInsideEnveloped (Recipient-Public-Key, Sender-Private-Key... address match using an algorithm described in [Mtag] that is based on a server specific **secret key** . This means that the attackers cannot forge new download URLs, they can only replay ones...email address of the client. The first part of the response will be the private **keys** . The **second** part of the response will be a certificate chain that starts with the user 1...

...Public-Key-Length - n bytes, MSB first = length of following field in bytes.

* Enveloping-Public- **Key** - n bytes, MSB **first** = Modulus.

The format of the Certificate Response is shown below. In another preferred embodiment, the...transformation of the fields of a Resource Tag can be based on one or more **secret keys** known to the Resource Owner using series of block encryption steps on portions of the...

...allows the transformation to be reverse by an entity that knows the one or more **secret . keys** .

For a 9 to 16 byte Resource Tag, the cryptographic transformation can be performed by...

...that the User (client) communicating with the Resource Owner (server) has current access to a **secret key** (e.g., triple-DES or XTEA or RC5 or AES key) associated with a key...the User Credential Information where the key identifier allows the server to lookup the same **secret key** known to the client, and other fields in the User Credential Information are verified@ using a cryptographic checksurn based on that same **secret key** .

The Resource Owner determines whether to grant access to the Resource (e.g., e-mail...

...embodiment (16), wherein the fields of a Resource Tag are based on one or more **secret keys** known to the Resource Owner. (19) The method in

46 The method in claim 6, wherein the first information comprises the Resource Tag, and...wherein the cryptographic primitives for Encrypted-Data providing privacy and data integrity based on a **secret key** and a cipher algorithm.

91 The method in claim 90, wherein the cipher algorithm being...

...claim 89, wherein the cryptographic primitives for Signed-inside-Enveloped-Data providing transport of a **secret key** from Sender to Recipient using a public key of the recipient.

93 The method in claim 92, wherein the **secret key** being selected from the set comprising a message key and a session key. . The method...
...wherein the cryptographic primitives for Encrypted-Data providing privacy and data integrity based on a **secret key** and a cipher algorithm; and the cryptographic primitives for Signed-Inside-Enveloped-Data providing transport of a **secret key** from Sender to Recipient using a public key of the recipient.

96 The method in...

...wherein the cryptographic primitives for Encrypted-Data providing privacy and data integrity based on a **secret key** and a cipher algorithm.

99 The method in claim 90, wherein the cipher comprise a...the next block of Encrypted Data. 1 00. The method in claim 99, wherein the **secret key** to the cipher is one input to this primitive. 101. The method in claim 99...

...cipher without an Initialization Vector, the bytes of the key are not reused, and the **secret key** to the cipher is one input to this primitive. 103. The method in claim 102...

...tamper detection, is provided by a cryptographic message authentication code that is based on a **secret key** . . The method in claim 104, wherein the secret is equal to or derived from the...

...122. The method in claim 89, wherein new secret session keys are derived from old **secret keys** that where previously agreed to by the Sender and Recipient thereby avoiding all or a...wherein the Secure Response message protocol is implemented using the Encrypted-Data primitive with a **secret key** know to the Recipient that is included inside the message that was received securely. 138...

...wherein the Secure Response message protocol is implemented using the Encrypted-Data primitive with a **secret key** know to the Recipient that is included inside the message that was received securely and...claim 156, wherein the cryptographic primitives for Signed-Inside-Enveloped-Data provide transport of a **secret key** from Sender to Recipient using a public key of the recipient. 158. The method in...

14/3,K/51 (Item 9 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00841904 **Image available**
DIGITAL RIGHTS MANAGEMENT WITHIN AN EMBEDDED STORAGE DEVICE

GESTION NUMERIQUE DE DROITS DANS UN DISPOSITIF DE MEMOIRE INTEGRE
Patent Applicant/Assignee:
DATAPLAY INC, 2560 55th Street, Boulder, CO 80301-5706, US, US (Residence), US (Nationality)
Inventor(s):
LEE Lane W, 894 S. Bermont Drive, Lafayette, CO 80026, US,
ZAHARRIS Daniel R, 7329 Mt. Meeker Road, Longmont, CO 80503, US,
Legal Representative:
STEUBER David E (et al) (agent), Skjerven Morrill MacPherson LLP, 25 Metro Drive, Suite 700, San Jose, CA 95110, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200175562 A2-A3 20011011 (WO 0175562)
Application: WO 2001US10405 20010329 (PCT/WO US0110405)
Priority Application: US 2000542510 20000403
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 9881

Main International Patent Class: **G06F-001/00**
Fulltext Availability:
Detailed Description

Detailed Description
... code or key to access multiple media, and presents a potential for interception of enabling **keys** or **codes** .

Many previous **distribution** systems, especially those relating to electronically or optically stored information, have been designed to prevent...the storage medium by the data storage engine. The keys may be encrypted using a **secret key** stored within the data storage engine prior to writing them to the media. In stage...

14/3,K/52 (Item 10 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00757055 **Image available**
PUBLIC CRYPTOGRAPHIC CONTROL UNIT AND SYSTEM THEREFOR
UNITE DE CONTROLE CRYPTOGRAPHIQUE PUBLIQUE ET SYSTEME DE MISE EN OEUVRE
Patent Applicant/Assignee:
WAVE SYSTEMS CORP, Suite B200, 480 Pleasant Street, Lee, MA 01238, US, US (Residence), US (Nationality)
Inventor(s):
SPRAGUE Steven K, 147 Reservoir Road, Lenox, MA 12040, US
KAZMEIRCZAK Gregory J, 36 Labaw Way, Belle Mead, NJ 08502, US
Legal Representative:
JACOBSON Allan J, Intellectual Property Law, 13310 Summit Square Center, Route 413 & Doublewoods Road, Langhorne, PA 19047, US
Patent and Priority Information (Country, Number, Date):

Patent: WO 200070429 A1 20001123 (WO 0070429)
Application: WO 2000US13239 20000515 (PCT/WO US0013239)
Priority Application: US 99313295 19990517
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AU CA CN JP KR NO
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Publication Language: English
Filing Language: English
Fulltext Word Count: 12612

Main International Patent Class: **G06F-001/00**
Fulltext Availability:
Detailed Description
Claims

Detailed Description
... 8 parity
bits.

As used herein, performing a cryptographic operation on a variable under a **secret key** means to encrypt (or decrypt) that variable (usually a key) using the **secret key** to generate another key. Encryption may be performed under a
single key, or under multiple...on a first fixed string A 940, a second fixed
string B 956 and a **secret key** , called the client key 942. The client key 942 is stored in a programmable memory...

Claim
... generating a first security applet and encrypting said first security applet in process using a **first** cryptographic **key** to form a **first encrypted** security applet and **distributing** said first **encrypted** security applet to said user computer,
a cryptographic key distribution method at said cryptographic operations process using a **first** cryptographic **key** to form a **first encrypted** security applet and **distributing** said first **encrypted** security applet to said user computer, a cryptographic key distribution apparatus at said cryptographic operations...

14/3,K/53 (Item 11 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00557577 **Image available**
DISTRIBUTING ACCESS TO A DATA ITEM
REPARTITION DE L'ACCES A UN ARTICLE DE DONNEES
Patent Applicant/Assignee:
GLASSBROOK INC,
Inventor(s):
KAWELL Leonard M Jr,
DIAZ Thomas R,
HEINEN Mary Ellen,
HEINEN Rodger J Jr,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200020950 A1 20000413 (WO 0020950)
Application: WO 99US23474 19991007 (PCT/WO US9923474)
Priority Application: US 98167888 19981007

Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZW GH GM KE LS MW SD SL SZ TZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 8069

Main International Patent Class: **G06F-001/00**
Fulltext Availability:
Detailed Description
Claims

Detailed Description
... to the data item. At least one of the transfers of permission may include the **transfer** of a **first encryption key** , and the method may include using a **second** encryption **key** to encrypt the **first encryption key** prior to **transfer** . The **first encryption key** may include a **secret**
key and the second encryption key may include one of the keys in a public/private...each of the sender computers and recipient computers may rely on encryption devices known as **secret keys** and public/private key sets, and may include a highly secure mechanism, which may handle...
...more of the keys or key sets, or encrypted or unencrypted data, or both. A **secret key** (also known as a symmetric key) is a s tri ng of data (e.g...

...in a way that allows the other data to be de-encrypted using the same **secret key** . A public/private key set includes two strings of data (e.g., 1024 bits each...

...Security Dynamics, Inc., 1982.

A conventional general-purpose computer can be used to generate the **secret key** and the public/private key set, which can be stored in conventional computer files, as...

...implement a public/private key encryptor 56, a public/private key cle-encryptor 58, a **secret key** encryptor 60, and a **secret key** de-encryptor 62. A permission data bank 64, a public key 66, a private key...

...known as Java.

In a specific embodiment, only the publisher computer is provided with a **secret key** encryptor (e.g., because the other computers are not originators of encrypted data items) and only the end-user computer is provided with the **secret key** de-encryptor (e.g., because the other computers do not display or otherwise make significant...

...Figs. 8-14 illustrate a detailed example 72 of the usage permission transfer procedure. A **secret key** 74 (e.g., a randomly-generated 40-bit number) is used to encrypt book data 76 to produce **secret key** encrypted book data 78 (step 2010), which is stored at a sender computer (step 2020). (In a specific embodiment, the **secret key** is also

14/3,K/54 (Item 12 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2005 WIPO/Univentio. All rts. reserv.

00418748 **Image available**
SYSTEMS AND METHODS FOR SECURE TRANSACTION MANAGEMENT AND ELECTRONIC RIGHTS PROTECTION
SYSTEMES ET PROCEDES DE GESTION DE TRANSACTIONS SECURISEES ET DE PROTECTION **DE DROITS ELECTRONIQUES**
Patent Applicant/Assignee:
INTERTRUST TECHNOLOGIES CORP,
Inventor(s):
GINTER Karl L,
SHEAR Victor H,
SIBERT W Olin,
SPAHN Francis J,
VAN WIE David M,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9809209 A1 19980305
Application: WO 97US15243 19970829 (PCT/WO US9715243)
Priority Application: US 96706206 19960830
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH HU IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZW GH KE LS MW SD SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 195626

Main International Patent Class: **G06F-001/00**
Fulltext Availability:
Detailed Description

Detailed Description
... over the use
of the invention's features. VDE also includes certain user
- 20 providers, **distributors** , and users.

Information **distributed** using VDE may take **many** forms.

It may, for example, be "distributed" for use on an individual's own computer...the
specific VDE installation and/or user), private key techniques such as triple DES to **encrypt** content, public **key** techniques such as RSA to protect communications and to provide the benefits of digital signature...assembly.

One of the load modules 1100b shown in this example is itself compnised of **plural** load modules 1100c, 1100d. Some of the load modules @ e. cr., 1 100a, 1 100d...

14/3,K/55 (Item 13 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00413443 **Image available**
PROTECTION OF DATABASE CONTENTS AGAINST USE WITHOUT PERMIT
PROTECTION DU CONTENU DE BASE DE DONNEES CONTRE DES UTILISATIONS NON AUTORISEES
Patent Applicant/Assignee:
SIGBJoRNSEN Sigurd,
HAGLUND Magne Arild,
OLESHCHUK Vladimir A,
Inventor(s):
SIGBJoRNSEN Sigurd,
HAGLUND Magne Arild,
OLESHCHUK Vladimir A,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9803904 A1 19980129
Application: WO 97NO185 19970717 (PCT/WO NO9700185)
Priority Application: NO 962997 19960718
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH HU
IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL
PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZW GH KE LS MW
SD SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH DE DK ES FI FR GB GR IE
IT LU MC NL PT SE BF BJ CF CG CI CM GA GN ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 8145

Main International Patent Class: **G06F-001/00**
International Patent Class: **G06F-17:30**
Fulltext Availability:
Detailed Description

Detailed Description
... card, for example, which may be denoted a master key, or be encrypted using the **secret key** , such as with symmetric cryptographic systems, e.g. DES. Only when the parameters are decrypted...admitted to more than one "information 1 5 layer" in the database (by authorization at **multiple** levels) the **keys** are **transferred** in **encrypted** form to the tamperproof unit which then decrypts the key data by means of the...

14/3,K/56 (Item 14 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00344642
SYSTEMS AND METHODS FOR SECURE TRANSACTION MANAGEMENT AND ELECTRONIC RIGHTS PROTECTION
SYSTEMES ET PROCEDES DE GESTION SECURISEE DE TRANSACTIONS ET DE PROTECTION ELECTRONIQUE DES DROITS
Patent Applicant/Assignee:
ELECTRONIC PUBLISHING RESOURCES INC,
Inventor(s):
GINTER Karl L,
SHEAR Victor H,
SPAHN Francis J,
VAN WIE David M,
Patent and Priority Information (Country, Number, Date):

Patent: WO 9627155 A2 19960906
Application: WO 96US2303 19960213 (PCT/WO US9602303)
Priority Application: US 95388107 19950213
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AL AM AT AU AZ BB BG BR BY CA CH CN CZ DE DK EE ES FI GB GE HU IS JP KE KG KP KR KZ LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK TJ TM TR TT UA UG UZ VN KE LS MW SD SZ UG AZ BY KG KZ RU TJ TM AT BE CH DE DK ES FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 207972

Main International Patent Class: **G06F-001/00**
International Patent Class: **G06F-17:60**
Fulltext Availability:
Detailed Description

Detailed Description
... in place
and/or by negotiation between concurrently proposed content control information submitted by a **plurality** of parties. A given model may be asynchronously and progressively modified over time in accordance...
?

15/TI/1 (Item 1 from file: 347)
DIALOG(R)File 347:(c) 2005 JPO & JAPIO. All rts. reserv.

METHOD AND DEVICE FOR MANAGING DATA

15/TI/2 (Item 2 from file: 347)
DIALOG(R)File 347:(c) 2005 JPO & JAPIO. All rts. reserv.

DATA MANAGEMENT SYSTEM

15/TI/3 (Item 3 from file: 347)
DIALOG(R)File 347:(c) 2005 JPO & JAPIO. All rts. reserv.

DATA COPYRIGHT MANAGEMENT DEVICE

15/TI/4 (Item 4 from file: 347)
DIALOG(R)File 347:(c) 2005 JPO & JAPIO. All rts. reserv.

DIGITAL INFORMATION MANAGEMENT APPARATUS

15/TI/5 (Item 5 from file: 347)
DIALOG(R)File 347:(c) 2005 JPO & JAPIO. All rts. reserv.

AUTHENTICATION SYSTEM

15/TI/6 (Item 6 from file: 347)
DIALOG(R)File 347:(c) 2005 JPO & JAPIO. All rts. reserv.

BICYCLE LOCKING DEVICE

15/TI/7 (Item 7 from file: 347)
DIALOG(R)File 347:(c) 2005 JPO & JAPIO. All rts. reserv.

REMOTE CONTROL LOCK

15/TI/8 (Item 8 from file: 347)
DIALOG(R)File 347:(c) 2005 JPO & JAPIO. All rts. reserv.

DATA CONTENTS DISTRIBUTION SYSTEM

15/TI/9 (Item 9 from file: 347)
DIALOG(R)File 347:(c) 2005 JPO & JAPIO. All rts. reserv.

COPYRIGHT MANAGING DEVICE

15/TI/10 (Item 10 from file: 347)
DIALOG(R)File 347:(c) 2005 JPO & JAPIO. All rts. reserv.

DATA COPYRIGHT MANAGEMENT SYSTEM

15/TI/11 (Item 11 from file: 347)
DIALOG(R)File 347:(c) 2005 JPO & JAPIO. All rts. reserv.

DATA COPYRIGHT MANAGEMENT DEVICE

15/TI/12 (Item 1 from file: 350)
DIALOG(R)File 350:(c) 2005 Thomson Derwent. All rts. reserv.

Key management method for use in data copyright **management system, involves** decrypting copyrighted **primary data to plain text using primary use permit key, and receiving secondary use permit key for editing data**

15/TI/13 (Item 2 from file: 350)
DIALOG(R)File 350:(c) 2005 Thomson Derwent. All rts. reserv.

Digital content copyright protecting system for electronic commerce, provides crypt key for encrypting, decrypting, re-encrypting or re-decrypting contents while performing encrypting/re-encrypting of contents

15/TI/14 (Item 3 from file: 350)
DIALOG(R)File 350:(c) 2005 Thomson Derwent. All rts. reserv.

Data content dealing method in data management system, involves transferring encrypted editing scenario and secret key to other user, where it is further decrypted to reconstitute edited data content

15/TI/15 (Item 4 from file: 350)
DIALOG(R)File 350:(c) 2005 Thomson Derwent. All rts. reserv.

Copyright control system for use with computer - encrypts or decrypts **information using key obtained from** copyright **control centre for primary utilisation of encrypted digital** information

15/TI/16 (Item 5 from file: 350)
DIALOG(R)File 350:(c) 2005 Thomson Derwent. All rts. reserv.

Data copyright management system using key distribution for transfer to secondary user - has key control centre and uses primary copyright label and primary use permit key, latter including first encryption key for primary data, second encryption key for editing data and third key for secondary use

15/TI/17 (Item 6 from file: 350)
DIALOG(R)File 350:(c) 2005 Thomson Derwent. All rts. reserv.

Crypt key system esp. for copyright protection or management in television broadcasting or online database - uses secret key and public key encryption methods as well as digital signature with crypt keys supplied through broadcast being optionally encrypted

15/TI/18 (Item 7 from file: 350)
DIALOG(R)File 350:(c) 2005 Thomson Derwent. All rts. reserv.

Copyright control method for encrypted digital data for database system - adding utilisation permit key to digital data to allow user to decrypt data and process it in accordance with display, edit, storage, copy and transfer permit parts

15/TI/19 (Item 1 from file: 348)
DIALOG(R)File 348:(c) 2005 European Patent Office. All rts. reserv.

Key management method and apparatus
Verfahren und Gerat zur Schlusselverwaltung
Procede et dispositif pour la gestion de cles

15/TI/20 (Item 2 from file: 348)
DIALOG(R)File 348:(c) 2005 European Patent Office. All rts. reserv.

Method for data copyright control
Verfahren zur Steuerung der Datenurheberrecht
Procede de controle du droit d'auteur de donnees

15/TI/21 (Item 3 from file: 348)
DIALOG(R)File 348:(c) 2005 European Patent Office. All rts. reserv.

METHOD AND DEVICE FOR PROTECTING DIGITAL DATA BY DOUBLE RE-ENCRYPTION
VERFAHREN UND VORRICHTUNG ZUM SCHUTZ DIGITALER DATEN MITTELS DOPPELTER WIEDERVERSCHLUSSELUNG
PROCEDE ET DISPOSITIF DESTINES A PROTEGER DES DONNEES NUMERIQUES PAR DOUBLE RECRYPTAGE

15/TI/22 (Item 4 from file: 348)
DIALOG(R)File 348:(c) 2005 European Patent Office. All rts. reserv.

Digital copyright management system using electronic watermark
Urheberrechtsdatenverwaltungssystem mit elektronischem Wasserzeichen
Systeme de gestion de donnees de droits d'auteurs avec une filigraine electronique

15/TI/23 (Item 5 from file: 348)
DIALOG(R)File 348:(c) 2005 European Patent Office. All rts. reserv.

Data copyright management system and apparatus
Dateiurheberrechte-Verwaltungssystem und -vorrichtung
Systeme et dispositif de gestion de droits d'auteur de donnees

15/TI/24 (Item 6 from file: 348)
DIALOG(R)File 348:(c) 2005 European Patent Office. All rts. reserv.

Data content dealing system
System zum Behandeln von Dateninhalten
Systeme de transaction de contenu de donnees

15/TI/25 (Item 7 from file: 348)
DIALOG(R)File 348:(c) 2005 European Patent Office. All rts. reserv.

Secure data management system
Gesichertes Datenverwaltungssystem
Systeme securise de gestion de donnees

15/TI/26 (Item 8 from file: 348)
DIALOG(R)File 348:(c) 2005 European Patent Office. All rts. reserv.

Copyright control system
Urheberrechtskontrollsystem
Systeme de controle de droits d'auteur

15/TI/27 (Item 9 from file: 348)
DIALOG(R)File 348:(c) 2005 European Patent Office. All rts. reserv.

System for data copyright management using key distribution
System zur Datenurheberrechtsverwaltung unter Verwendung von Schlusselverteilung
Systeme de gestion de droits d'auteur de donnees utilisant une distribution de cle

15/TI/28 (Item 10 from file: 348)
DIALOG(R)File 348:(c) 2005 European Patent Office. All rts. reserv.

Crypt key system for secure electronic transactions
Verschlusselungssystem fur sichere elektronische Transaktionen
Systeme de cryptage pour des transactions electroniques securisees

15/TI/29 (Item 11 from file: 348)
DIALOG(R)File 348:(c) 2005 European Patent Office. All rts. reserv.

Apparatus for data copyright management system
Gerat fur Dateiurheberrechte-Verwaltungssystem
Appareil pour systeme de gestion de droits d'auteur de donnees

15/TI/30 (Item 12 from file: 348)
DIALOG(R)File 348:(c) 2005 European Patent Office. All rts. reserv.

Data copyright management system
Urheberrechtsdatenverwaltungssystem
Systeme de gestion de donnees de droits d'auteurs

15/TI/31 (Item 13 from file: 348)
DIALOG(R)File 348:(c) 2005 European Patent Office. All rts. reserv.

Data copyright management system
Datenurheberrechtsverwaltungssystem
Systeme de gestion des droits d'auteur de donnees

15/TI/32 (Item 14 from file: 348)
DIALOG(R)File 348:(c) 2005 European Patent Office. All rts. reserv.

Method for controlling copyright **of** encrypted **digital data**
Verfahren um die Urheberrechte von verschlusselten numerischen Daten zu kontrollieren
Procede pour controler les droits d'auteur de donnees numeriques chiffrees

15/TI/33 (Item 1 from file: 349)
DIALOG(R)File 349:(c) 2005 WIPO/Univentio. All rts. reserv.

SYSTEM FOR PROTECTING BOTH COPYRIGHTS AND FAIR-USE RIGHTS AT THE SAME TIME
SYSTEM FOR PROTECTING BOTH COPYRIGHTS AND FAIR-USE RIGHTS AT THE SAME TIME
SYSTEME PROTEGEANT EN MEME TEMPS A LA FOIS LES DROITS D'AUTEUR ET LES DROITS D'UTILISATION EQUITABLE

15/TI/34 (Item 2 from file: 349)
DIALOG(R)File 349:(c) 2005 WIPO/Univentio. All rts. reserv.

SECURE DISTRIBUTION OF DIGITAL REPRESENTATIONS
DISTRIBUTION SECURISEE DE REPRESENTATIONS NUMERIQUES
?